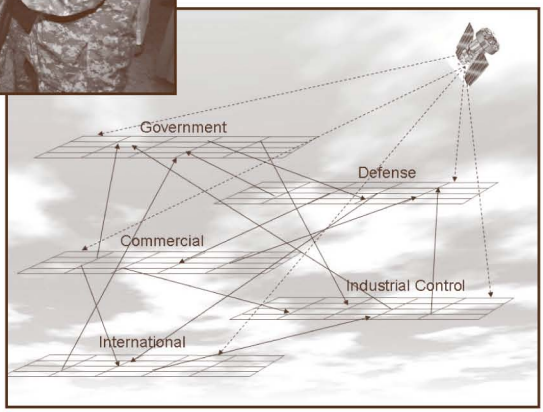

INFORMATION AS POWER

AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE STUDENT PAPERS

VOLUME 4

Edited by
Jeffrey L. Caton, Cori E. Dauber,
Jeffrey L. Groh, and David J. Smith

INFORMATION IN WARFARE GROUP, U.S. ARMY WAR COLLEGE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information as Power. Volume 4. An Anthology of Selected United States Army War College Student Papers	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army War College,122 Forbes Avenue,Carlisle,PA,17013**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**196**	

US ARMY WAR COLLEGE

INFORMATION AS POWER

VOLUME 4

AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE STUDENT PAPERS

Information as Power is a refereed anthology of United States Army War College (USAWC) student papers related to information as an element of national power. It provides a medium for the articulation of ideas promulgated by independent student research in order to facilitate understanding of the information element of power and to better address related national security issues. The anthology serves as a vehicle for recognizing the analyses of Army War College students and provides a resource for USAWC graduates, senior military officers, and interagency national security practitioners concerned with the information element of national power.

Special thanks to David J. Smith for his significant editorial and administrative support, to Ritchie Dion for his meticulous layout editing, and to Jennifer Nevil for the cover design.

Information as Power


Prudens
Futuri

INFORMATION AS POWER

An Anthology of Selected United States Army War College Student Papers

Volume Four

Editors:

Jeffrey L. Caton, Cori E. Dauber,
Jeffrey L. Groh, David J. Smith

Information as Power

An Anthology of Selected United States Army War College Student Papers

Volume Four

Executive Agent for the Anthology:
United States Army War College

Published January 2010.

This publication is available on line at the following:

http://www.carlisle.army.mil/dime or,
http://www.csl.army.mil/InfoAsPower.aspx

Cover photograph by Staff Sgt. DeNoris A. Mickle, USAF.
Used by permission.

U.S. ARMY WAR COLLEGE
CARLISLE BARRACKS, PENNSYLVANIA 17013

Contents


Prudens
Futuri

Preface

The Information in Warfare Working Group (I2WG) of the U.S. Army War College (USAWC) is pleased to present this anthology of selected student work from Academic Year 2009 representing examples of well-written and in-depth analyses on the vital subject of Information as Power. This is the fourth volume of an effort that began in 2006. The I2WG charter calls for it to coordinate and recommend the design, development and integration of content and courses related to the information element of power into the curriculum to prepare students for senior leadership positions. This publication is an important component of that effort.

Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents, to include the 2007 National Strategy for Strategic Communication and Public Diplomacy, allude to different aspects of information but without a holistic, overarching strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power…and that information is woven through the other elements since their activities will have an informational impact.[2] Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[3] Information as power is wielded in a complex environment consisting of the physical, informational, and cognitive dimensions.

The current information environment has leveled the playing field for not only nation states, but non-state actors, multinational corporations and even individuals to affect strategic outcomes with minimal information infrastructure and little capital expenditure. Anyone with

a camera cell phone and personal digital device with internet capability understands this. Adversary use of information as an asymmetric strategic means has been extremely effective in the current theaters of Iraq and Afghanistan leading Richard Holbrooke to famously muse: "How can a man in a cave out-communicate the world's leading communications society?"[4] And so, while the United States is certainly a military "superpower" whether it maintains that same status with regard to information is debatable.

On the other hand, the U.S. military has increasingly leveraged advances in information infrastructure and technology to gain advantages on the modern battlefield. One example from Operation Iraqi Freedom is the significant increase in situational awareness from network centric operations that enabled the military to swiftly defeat Iraqi forces in major combat operations.[5]

Clearly, managing the "message" while controlling and exploiting the necessary technological "means" represent critical challenges in today's information environment. We hope that this anthology will serve not only to showcase the efforts of the College but to inform the broader body of knowledge as the Nation considers how best to operate effectively and proactively within this environment while countering current and potentially future adversaries.

Professor Dennis M. Murphy
Chair, Information in Warfare Working Group
United States Army War College

Section One

Information Effects in the Cognitive Dimension


Prudens
Futuri

Introduction

Dennis M. Murphy
Professor of Information in Warfare
Center for Strategic Leadership
U.S. Army War College

This section focuses on "information effects" that include those actions, images, and words that ultimately influence perceptions and attitudes leading to a change in behavior. Rafal Rohozinski and Dennis Murphy rightly note that "if IO (information operations) is meant to accomplish a planned intent, then the concept of 'information effects' compels a broader analytical lens that includes the unintended consequences of both IO and kinetic actions." The Department of Defense (DoD) later included this same explanation in their description of the concept of strategic communication. In short, the messages soldiers and U.S. government officials send, both through informational means and other actions, will in some way influence the receivers: adversary, friendly, and neutral; foreign and domestic. This section considers strategic communication as a way to achieve these information effects. Public Diplomacy, military Information Operations and Public Affairs are inherently capabilities (means) of strategic communication and are explicitly stated as such in nascent DoD literature on this topic. The papers in this section grapple with some of the issues present in these capabilities and the ability of the United States to use them effectively to achieve strategic objectives.

Colonel Jeffrey L. Scott examines the requirement for and the role of speed and accuracy in informing and influencing key audiences. His paper provides an overview of how the enemy uses information; the enemy's strategy to disrupt U.S. operations; and the application of current decision making processes in defeating the enemy's strategy. It concludes with a recommendation for an information strategy developed to overcome the speed versus accuracy dilemma and increase operational effectiveness.

Colonel David P. Anders considers the role of strategic communication in counterinsurgency operations, offering a model to operationalize the concept. He argues that strategic communication should be made a priority by directing it be a line of operation on equal footing with security, governance, and development within the counterinsurgency spectrum thus ensuring continuous strategic, operational and tactical leadership attention and input. The steps in developing this offensive model can be identified by answering the "five W's" (why, who, where, what, when), and most importantly the "how" of the counterinsurgent strategic communication environment.

Lieutenant Colonel Douglas W. Little explores how U.S. hubris regarding its global influence in a unipolar world marginalized a once independent and effective Department of State public diplomacy effort. Similarly, the paper illustrates how a misguided U.S. impression of the universality of the democratic peace theory and a fundamental misunderstanding of the roots of international terrorism continue to impede sustainable progress in the war of ideas. The paper concludes with recommendations to revitalize U.S. public diplomacy and to establish a sustainable and effective vision for the future.

Finally, Colonel Suhail M. Alseraidi of the United Arab Emirates provides a fascinating conceptual look at what a U.S. National Communication Strategy should look like. Colonel Alseraidi, an International Fellow in the Army War College class of 2009, provides insights through the eyes of a partner nation and its own unique cultural lens on the appropriate approach to strategic communication with the world in this short, but important essay.

Well-written and insightful, these papers serve to inform the military and the nation as it continues to conduct military campaigns in two theaters while engaging the world.

Speed Versus Accuracy: A Zero Sum Game

Colonel Jeffrey L. Scott
United States Army

An effective information strategy requires credibility. Truthful and accurate messaging develops and maintains credibility, however, the collection of correct information required for accurate messaging sacrifices speed. Speed is required to provide current, relevant information to inform and influence key populations. The sacrifice in speed to release messages results in the inability to "tell your side of the story" first. Constantly disputing initial published accounts reduces the ability to effectively inform and influence select key audiences, and over time reduces source and message credibility. The dilemma of speed versus accuracy in messaging creates a zero sum game in information strategy that reduces operational effectiveness.

This paper examines the trade-offs between speed and accuracy in an irregular warfare information environment. It begins by establishing the requirement for, and the roles of, speed and accuracy in informing and influencing key audiences. The paper provides an overview of how the enemy uses information, the enemy's strategy to disrupt U.S. operations, and the application of Boyd's OODA loop in defeating the enemy's strategy. It concludes with a recommendation for overcoming the speed versus accuracy dilemma through developing and implementing an effective information strategy in which "actions and words" are congruent, ensuring the accuracy and speed required to inform and influence key populations.

In March 2006, U.S. and Iraqi Special Forces engaged and defeated a Jaish al Mahdi (JAM) force responsible for the murders of several Iraqi civilians and Iraqi Soldiers. Within an hour of leaving the engagement site, JAM had staged the bodies of dead fighters to appear as civilians, photographed the scene, and posted the images on the web along with a press release claiming U.S. forces had killed the men while they prayed in a mosque. Although U.S. forces photographed and videotaped the action, it took three days to release the information.[1] The untimely U.S.

release of information appeared as a reaction to enemy propaganda and resulted in loss of credibility for the U.S. effort.

In July 2008, U.S. led coalition forces in Afghanistan stated they conducted an airstrike which killed insurgents.[2] Locals claimed the air strike killed civilians. An investigation revealed the airstrike killed 47 civilians attending a wedding party.[3] The speed of response by the U.S. forces resulted in inaccurate statements being made before the facts of the situation were fully known. The dissemination of misinformation damaged U.S. credibility and gave the enemy an opportunity to exploit against the U.S. effort.

In both examples, the misapplication of speed in disseminating information to key audiences damaged the credibility of the U.S. mission. With the importance of information in today's irregular warfare environment, how do you develop an effective strategy to overcome the speed versus credibility dilemma? An effective information strategy is based on decentralization. Operations planned and conducted and the daily interactions of the units and Soldiers on the ground must send the message. Only then can an information strategy maintain the speed to enable and enhance action and bolster the organization's credibility due to enhanced operational effectiveness.

Credibility and Speed

Accuracy is essential to an effective information strategy. Many simply believe presenting factual information guarantees credibility. However, does accuracy equal credibility? Credibility is a condition based upon the audiences' perceptions of the message and source.[4] Is the organization trustworthy and is the message believable?

The audience considers three factors in determining credibility: accuracy of message content, unbiased presentation, and the audience's reaction to the source.[5] Any verified or perceived error in information presented is viewed as inaccuracy. Presenting only one point of view of the issues or omission of unfavorable information is considered bias. The audience's reaction to the source is based on the audience's past and present experiences (both actual and perceived) with the source.[6] As a condition, credibility must be developed and maintained by the source

with the audience. Because it must be developed and maintained with the audience, credibility must be oriented toward action and not based solely on words.

Credibility is developing the "cores of credibility" – integrity, intent, capability, and results – that make the communicator and the communicator's message believable with key populations.[7] In *Speed of Trust*, Stephen Covey goes to great lengths to explain the "cores of credibility" because they are the essence of developing and maintaining the condition of credibility.[8] Integrity is more than just honesty and a reputation of being truthful. It is being congruent with actions and words. Intent involves transparency – no hidden agendas or motives. Intent is derived from the behavior of the organization and is directly related to integrity. The audience must believe the organization has their interest in mind. Capabilities are displayed through professionalism (expertise and knowledge) of the organization. Lastly, the organization produces results. They are operationally effective. The organization is perceived by the audience to finish what it starts.[9] The application of or lack of adherence to these "cores of credibility" in all actions with the audience determines their past and present experiences either positive or negative. As stated earlier, these experiences determine the audience's reaction to the organization as a source – whether it is trustworthy and their message believable.

In determining the quality and credibility of information, timeliness of information is required to ensure it is relevant to the audience. The requirement for currency, and the fact technology accelerates information delivery to the audience, makes speed an important component of information strategy. It is essential to release information to inform audiences of one's positive actions with sufficient speed to prevent the enemy from exploiting and discrediting one's action through the use of misinformation and disinformation.

Speed is important when reporting unfavorable news resulting from the actions of friendly forces. Releasing factual information related to negative events prevents the negative credibility which results from allowing the enemy to release the information first. Failure to apply speed in releasing news of negative action gives the appearance of a cover up, a lack of transparency. It enhances the effectiveness of enemy

propaganda by allowing him to release the information first. The delayed release by friendly forces either becomes an endorsement, or confirms the accuracy of the enemy's information thereby increasing their credibility.[10]

Speed is most commonly associated with, and seen as a requirement in, crisis response communications. A crisis is "a significant threat to operations that can have negative consequences if not handled properly."[11] A crisis causes an information vacuum. In crisis response, speed is required to allow the organization to tell its side of the story and fill the information void before the enemy can do so with misinformation or disinformation. However, there are factors limiting the application of speed in responding to a crisis event. The size of the incident, the amount of confusion created by the incident, the location of the incident, and the ability to respond to the incident scene all affect the ability to collect the factual information required to quickly inform audiences of the incident.[12]

In February 2007, an incident in Afghanistan provided an example of the risk associated with applying speed in response to a crisis event without collecting and confirming the facts and de-conflicting the message within the organization. A suicide bomber attacked a Khost hospital opening ceremony. Different U.S. elements and the local media participating in the ceremony immediately began to disseminate different accounts of the event. After several weeks of attempting to correct the initial misinformation disseminated, the end result remained unchanged. The local audience perceived the United States to have intentionally spread disinformation concerning the event.[13]

Dissemination of inaccurate information affects the "cores of credibility" of integrity, intent, and capability of the organization. Inaccurate information damages the organization's reputation of truthfulness and results in incongruence between actions and words. It makes the organization look inconsistent and displays a lack of transparency. Disseminating inaccurate information requires retractions and corrections which in turn make the organization look incompetent.[14] This does not mean speed should be sacrificed to mitigate the risk to credibility.

In *Ongoing Crisis Communication: Planning, Managing, and Responding*, Timothy W. Coombs presents instances in which speed in crisis response displayed control of the situation. He explains how a quick response demonstrates the organization is taking action and is capable while a slow one displays incompetence.[15] The proper application of speed in response demonstrates competence and increases the capability element of the "cores of credibility."

The proper application of speed and its affect on credibility is not limited to crisis response. As discussed, it holds true for all situations related to an effective information strategy. This is the zero sum game of speed and accuracy in information strategy. In irregular warfare, this is the vulnerability the enemy attacks.

The Enemy's Strategy

In irregular warfare, the enemy understands he cannot defeat the military forces of the stronger opponent. Destroy the stronger forces' credibility and he destroys their ability to inform and influence key audiences in order to maintain the support necessary to succeed. This is the intent of the enemy's strategy.[16] In order to fulfill this strategic intent and keep their message in front of supporters and opponents alike, the enemy relies on action in the form of terrorism and intimidation. These are acts of violence conducted by the enemy to influence audiences' perceptions, cognitions, and actions.[17] In *The Accidental Guerrilla*, David Kilcullen labeled this use of physical action to achieve information effects as "armed propaganda."[18] These violent acts have little military value but send a message to the enemy's target audiences – their supporters and opponents. Because negative information more easily influences than positive, these negative events have a greater impact.[19] Additionally, because the enemy controls the time, place, and manner of the violent acts, it increases their credibility as a source and provides a level of legitimacy with the audience.[20] "Armed propaganda" gains and maintains active and passive support of the population they are fighting for, erodes the political will of the opponent, and separates the opposing decision makers from the populace.[21] If terrorism and intimidation are designed to send a message, the media is the messenger.

Richard Josten states "terrorism is strategic communication in the purest definition – message and action – utilizing the global communications network more to influence than inform."[22] Without the media, the enemy's "armed propaganda" would be ineffective. It would not reach its target audiences. The question to be answered is why are national and international media so quick to disseminate the enemy's message? Just as negative information is more apt to influence than positive information, violent action makes better news than peaceful, orderly behavior. According to Pratkanis and Aronson,

> *…editors and reporters tend to look for stories that 1) are new and timely, 2) involve conflict or scandal, 3) concern the strange or unusual, 4) happen to famous or familiar people, 5) capable of being made dramatic and personal, 6) simple to convey in a short space or time, 7) contain visual elements and, 8) fit a theme that is currently prominent in the news and society.*[23]

The enemy has become adept at exploiting the media. The Taliban's media campaign drives the news media and commands headlines creating the perception they are stronger than they really are.[24] Their spectacular attacks gain media headlines and facilitate their immediate response to journalists to shape the story to their advantage.[25] The Taliban outpace the Afghan government in accessibility and speed towards the media. They make regular calls and send text messages to journalists, often within minutes of attacks, to publicize their actions.[26]

This "speed strategy" utilized by the Taliban makes use of gate keeping, priming, and framing.[27] Gatekeeping involves intimidating community leaders and journalists in order to prevent them from making statements and reporting actions unfavorable to their cause or not giving them due prominence in the media. Priming involves the timing of "armed propaganda" to ensure the correct amount of space and time in the media is devoted to their message. It allows them to command the headlines in the media. This forces the audiences to focus on their issue and think about their message. The constant contact and immediate availability to journalists allow the Taliban to frame the information in such a way that it will influence the audience with the "facts" they provide.

The use of "armed propaganda" and "speed strategy" increases the enemy's ability to control operational tempo and places U.S. forces in a reactionary posture.[28] Constantly being in a reactionary posture leads to the loss of initiative which in turn reduces operational effectiveness. "Armed propaganda" and "speed strategy" attack credibility – the intent of the enemy strategy – by reducing the opponent's operational effectiveness.

Boyd's OODA Loop

Many attempt to apply John Boyd's OODA (Observe, Orient, Decide, Act) loop in response to the enemy's "armed propaganda" and "speed strategy." The application of the OODA loop is not incorrect in this environment. It is just the application of the wrong OODA loop concept developed by Boyd – his idea of the rapid OODA loop – for the situation (see figure 1). Boyd's intent of the rapid OODA loop is to increase speed in decision making and execution of kinetic action at the tactical level.[29] Tactical engagements require immediate action and results.

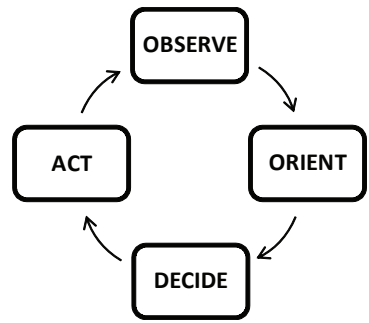

Figure 1: Traditional Rapid OODA Loop

In the information environment, the immediate response to a specific instance of "armed propaganda" is the release of public information. The application of speed in releasing public information involves providing the facts required to facilitate public safety to the media. This limits the enemy's ability to frame the "facts" of the incident with misinformation and disinformation and increases one's credibility by showing control over the situation as well as concern for the local populace. Because the organization reacts to a specific event which is part of an overall strategy designed to influence, it is impossible to counter the way the specific event has influence after the fact. It is the same as directly refuting each piece of enemy propaganda produced.[30] One cannot "out-loop" and disrupt the enemy's OODA loop by applying the rapid OODA loop in a reactionary state. The application

of the rapid OODA loop in this environment causes a trade-off between speed and accuracy of information resulting in the inability to develop and maintain credibility. By pursuing this course of action, the enemy's use of "armed propaganda" and "speed strategy" disrupts his opponent's ability to produce long term effects. The opponent is in a constant reactionary state and cedes the initiative to the enemy. The application of the OODA loop in effective information strategy goes beyond Boyd's idea of the rapid OODA loop to his later work concerning operational and strategic level strategies.

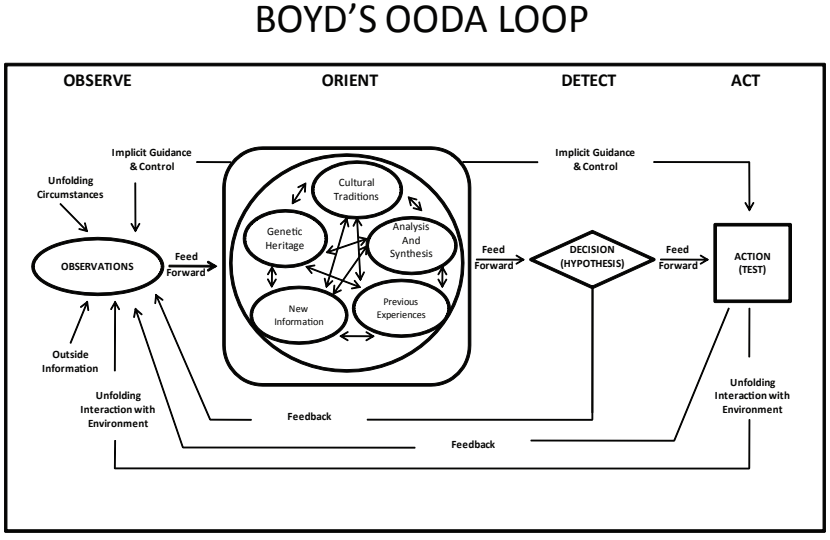

Figure 2: Boyd's OODA Loop[31]

Boyd later expanded the OODA loop theory to support his strategic perspective (see figure 2). As figure 2 depicts, Boyd's expanded OODA loop is much more detailed and complicated than his earlier rapid OODA loop concept. This expanded theory is based on interaction and isolation. Success depends on sustaining and improving the ability to interact within the operating environment and to isolate the enemy by limiting his ability to interact within that same environment.[32]

Boyd argues that interaction and isolation occur on three levels: physical, mental, and moral. Physical interaction occurs with the exchange of matter, energy, and information with others outside of the organization – friend and foe.[33] The physical includes both communication and

actions conducted with the outside world. Mentally an organization interacts by gathering and assessing the information from varying sources in order to develop mental images and impressions and matching those with the events occurring around the organization.[34] It is properly identifying positive and negative trends and changes to those trends in the environment which direct appropriate action. Moral interaction occurs by preventing mismatches in words and deeds. It is abiding by the "code of conduct and standards of behavior one is expected to uphold."[35] Sustaining and improving interaction with the environment is developing and maintaining credibility with key audiences.

Isolation limits the opponent's ability to sustain and improve his interaction with the environment. In the physical realm, he cannot gain support from others; mentally, he cannot make sense of his surroundings; morally, he fails to abide by the code of conduct or standards of behavior deemed acceptable.[36] The opponent is unable to develop and maintain credibility.

According to Boyd, interaction with the operating environment is a constant loop that begins with observation. Observation provides the information necessary for interaction in the mental realm. It is the primary source of new information which influences decisions and action. As part of the constant loop, observation collects feedback in the form of assessment of friendly actions including the reactions of the enemy and reactions and perceptions of key audiences. However, all this information is meaningless without proper orientation.

Boyd's expanded OODA loop places orientation in the central location, influencing all other elements of the loop. Orientation provides the vision, focus, and direction to process the information gathered by observation, and guide and control action.[37] It dictates one's ability to interact in the physical and moral realms. Orientation is the adaptive portion of the loop. ecause the environment is constantly changing, one's orientation must continue to grow, evolve, and adapt to interact with the environment. It detects changes in the environment and facilitates the necessary organizational adaptability to interact with the environment and operate within the opponent's OODA loop isolating him from the environment. Proper orientation facilitates speed in the

physical level but more importantly it allows one to set a tempo that isolates the opponent in the mental realm and limits the opponent's ability to adapt to the changing situation.[38]

Information Strategy

Irregular warfare doctrine, specifically counterinsurgency doctrine, stresses the importance of information and an indirect approach in winning and maintaining the support of key populations.[39] Current U.S. practice establishes Information Operations (IO) as a separate Line of Operation (LOO) or as a LOO encompassing all other LOOs.[40] The concept is correct – all action sends the correct message – but the application is incorrect. FM 3-24 describes all information requirements – public information, command information, expectation management, media engagement, influence operations, counter-propaganda, Soldier/leader interaction, etc. – as IO and activities within the IO LOO.[41] By definition and doctrine, IO, as a function, is an information activity designed to achieve specific effects – attack adversarial human and automated decision making and protect friendly forces' decision making – just as Psychological Operations (PSYOP) and Public Affairs (PA) are information activities designed to achieve specific effects in support of the operation.[42]

The misapplication of IO degrades the intended function of IO and limits the effectiveness and capabilities of other information activities by centralizing all information requirements under IO. Decentralization flattens the organization and increases operational effectiveness. Decentralization facilitates integrating all information activities into operational planning.[43] Properly placing information requirements back under the appropriate information activities allows access of those trained and responsible for planning and executing those activities to the planning process and the commander. Properly defining information strategy and applying it as the all-encompassing LOO would increase operational effectiveness and provide the decentralization required to properly employ all information activities in irregular warfare.

Defining information strategy as *the planning, coordination, and execution of kinetic and non-kinetic operations in conjunction with all information activities (strategic communication,*[44] *PA, PSYOP, and IO) in order to*

send a consistent message to key audiences enabling the achievement of the military and ultimately the political end facilitates decentralization and congruency in word and deeds. This decentralization and congruency would increase the speed of information dissemination and credibility of the organization increasing operational effectiveness.

Effective information strategy (see figure 3) is a continuous process of analysis, coordination, planning, execution, and assessment. Both kinetic and non-kinetic operations require utilizing Boyd's expanded OODA loop to be effective. All actions must be based on the proper observations and orientation. Information strategy must be pre-active, pro-active, and reactive.[45] Although depicted on the chart as being sequential stages, pre-active and pro-active are continuous, overlapping functions.

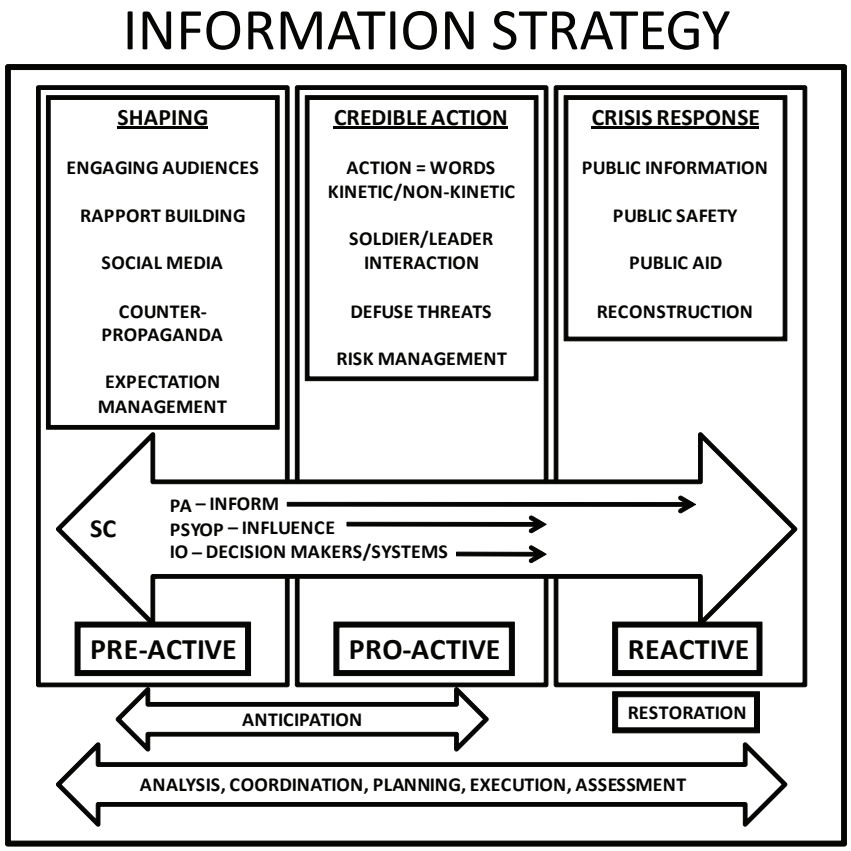

Figure 3: Information Strategy

Observation in the pre-active and pro-active stages identifies existing trends and changes to those trends within key audiences and in enemy activity. Proper orientation provides the flexibility and adaptability enabling effective exploitation, mitigation, and the ability to change established and developing trends in order to achieve the desired effects necessary to reach the military and political objectives. The pre-active and pro-active stages are designed to anticipate shock points in the established trends and limit the need for the reactive stage. Anticipation of shock points is not limited to potential events resulting from enemy action. The current civilian casualties situation in Afghanistan provides an excellent example of a shock point resulting from the action of U.S. forces. The initial incident in early 2007 which made international media headlines can be considered the actual shock point. All of the following events are related crisis events exploited by the enemy. These events continue to generate negative consequences to U.S. operations.

Pre-active activities encompass Boyd's three levels – physical, mental, and moral. The organization interacts with the environment to gather and assess information. It matches the information with on-going events and identifies trends and changes required to those trends to determine appropriate future action. Pre-active activities shape the environment in favor of the organization.

Engaging audiences, engaging media, and building rapport provide the social networking necessary to shape the information environment. Engaging audiences involves two-way communication creating stable relationships, not just selling the organization or its cause. Engaging the media establishes contact with journalists and facilitates accessibility of the organization to the media in such a manner they will seek out information from the organization. It is congruent with building rapport. Building rapport develops the "cores of credibility" of integrity, intent, and capability with each audience. This, coupled with "actions equal words" pro-active activities, develops and maintains the organization's credibility.

Social media is an emerging set of technologies utilized to disseminate information outside of mainstream media sources. The use of social media increases speed of information dissemination and interaction with key audiences. Social media, in the form of blogs, e-mail, and

sites such as YouTube, Facebook, Twitter, etc., decentralizes the responsibility of publishing information from organizations to the individual. Additionally, mainstream media is incorporating social media through their use of the sites listed above to encourage the "man on the street" to send information directly to local, national, and international news outlets. An effective information strategy must incorporate this technology into pre-active activities to inform and influence key audiences and maintain the initiative in the information environment. Implementation of this decentralized method of information dissemination will require efficient policies, training, and operational guidance to effectively use social media in information strategy.

Effective counter-propaganda does not get caught up in the reactive cycle of attempting to directly refute each piece of enemy propaganda. This reactive mentality only draws attention to the enemy's action and propaganda. Effective counter-propaganda will isolate the enemy from interacting with key audiences by discrediting the enemy as a source as well as his message. Identifying the enemy's propaganda themes enables counter-propaganda efforts to become part of planned Psychological Operations (PSYOP) programs and public information. Routine PSYOP products, public information, and Soldier interaction with key audiences should counter the enemy's themes without directly calling attention to the enemy's propaganda products. An excellent example of counter-propaganda is the routine release of messages from respected Muslims denouncing the extremist use of suicide bombers, the killing of innocent Muslims, and other atrocities carried out under the banner of Jihad. It attacks the enemy's theme of jihad, their legitimacy and creates a negative reaction in the audience when the atrocities are continued. It discredits the enemy with the key audiences.

Expectation management involves keeping all audiences informed of the actions and goals of friendly forces and the government. Transparency is a vital component of expectation management. Keeping the audiences informed limits rumors which feed the unrealistic expectations of the audiences. The organization must monitor perceptions and expectations of the populace and provide consistent messaging of future conditions and goals that do not exceed the abilities of the organization. Effective

expectation management supports the "cores of credibility" of intent, capability, and results.

Pro-active activities encompass Boyd's physical and moral levels. It is the physical interaction of the unit and the Soldiers with key audiences – the destruction of enemy forces, security operations, training partnered national security forces, infrastructure development, etc., as well as information. This Soldier/leader interaction, regardless of the mission, occurs whenever Soldiers are out in the populace. It is how they interact with and treat the populace while conducting operations. Pro-active activities establish the moral element of Boyd's three levels – the code of conduct and standards of behavior one is expected to uphold – essential for credibility. Pro-active activities maintain all the "cores of credibility."

Additionally, pro-active activities employ action and information to defuse threats to current positive trends and risk management to prevent crises. Defusing threats include actions taken to reduce the risk of the enemy creating a shock point in current trends or producing crises. Risk management consists of Rules of Engagement (ROE), Escalation of Force (EOF), and other policies implemented to limit negative perceptions and the creation of a crisis by friendly forces.

The reactive stage is only executed as a crisis response to a specific crisis. The purpose of the reactive stage is to restore order and maintain the credibility of the organization and mission. As stated earlier, crisis response deals primarily with dissemination of public information and action to ensure public safety. Speed in release of public information prevents the enemy from exploiting the event through the dissemination of misinformation and disinformation.

Conclusion

The trade-off between accuracy and speed in the information environment creates a zero sum game. Both are intertwined with the "cores of credibility" – integrity, intent, capability, and results – required to develop credibility with key audiences. Accuracy requires time to collect information sacrificing speed; speed sacrifices accuracy. Inaccuracy in information damages integrity, intent, and capability –

the message and source are untruthful, have hidden agendas, and the source is incompetent. Lack of speed damages intent and capability – implies a cover-up, a lack of transparency and incompetence due to lack of control.

Unable to defeat the military forces of the stronger opponent, the enemy attacks the counterinsurgent's credibility in order to limit his ability to gain and maintain the support of key audiences. The enemy's strategies of "armed propaganda" and "the speed strategy" exploit the speed versus accuracy dilemma. "Armed propaganda" and "the speed strategy" allow the enemy to control operational tempo and seize the initiative, and places U.S. forces in a constant reactionary state.

The misapplication of the rapid OODA loop by U.S. forces in reaction to a crisis will not "out-loop" and disrupt the enemy's OODA loop. Additionally, the centralization of all information requirements under the information activity of IO degrades the function of IO and limits the capabilities of other information activities. Application of Boyd's expanded OODA loop coupled with an information strategy that is pre-active and pro-active anticipates negative trends and potential shock points in positive trends and facilitates setting operational tempo and maintaining initiative. Defining information strategy as *the planning, coordination, and execution of kinetic and non-kinetic operations in conjunction with all information activities (strategic communication, PA, PSYOP, and IO) in order to send a consistent message to key audiences enabling the achievement of the military and ultimately the political end* facilitates decentralization and congruency in words and deeds. Decentralization of information activities creates a flatter organization allowing those responsible for planning and executing those activities access to the planning process and the commander. Because kinetic and non-kinetic operations planning and execution are conducted in conjunction with all information activities, the interaction of units and Soldiers on the ground and actions send the organization's message to key audiences. The application of information strategy at all operational levels (tactical, operational, and strategic) in this manner maintains the speed and accuracy to enable and enhance action and bolster the organization's credibility due to enhanced operational effectiveness.


Prudens
Futuri

Developing an Operational Strategic Communication Model for Counterinsurgency

Colonel David P. Anders
United States Army

The volatile, uncertain, complex, and ambiguous environment of the information age has accentuated the necessity of a strategic communication paradigm that can effectively articulate our national policies and interests.

United States (U.S.) military units are not sufficiently organized or trained to analyze, plan, and integrate the full spectrum of resources available to promote America's interests.[1] Military commanders at the theater strategic, operational, and tactical levels are nonetheless challenged with the vital task of how to successfully communicate information and ideas to multiple audiences, local and international, individually and simultaneously, as we fight in the counterinsurgencies of Iraq and Afghanistan.

Strategists in both wars agree with classic counterinsurgency (COIN) theorists that the real fight is for the support of the population, and that communication is essential to victory.[2] Of equal importance is ensuring that timely, accurate, and positive information concerning these wars is presented to the policy makers and citizens of the coalition partners participating in the wars with their national treasures and the blood of their soldiers. Unfortunately, the U.S. military has been historically ineffective in communicating accurate, truthful, and positive information to these populations and international target markets because of a failure to expedite information in a proactive manner. Consequently, the information initiative is lost and the result is a reaction to the enemy's disinformation strategy. The U.S. military has failed to achieve the desired information effects at the strategic, operational, and tactical levels due to a passive/reactive approach to Strategic Communication (SC).

Military doctrine does not adequately address this challenge. The enemy is acutely skilled at exploiting the 24/7 news cycle to exaggerate, twist, and distort the truth in order to discredit the host nation government and villainize coalition and U.S. forces in the eyes of the local population, the Muslim people, and the international media. Al Qaeda understands that today's information age has fundamentally changed not only the speed of how people communicate, but also how people form their opinions.[3] All the enemy needs is an event, not facts, to exploit their message. Abu Ghraib is a painful example of how a tactical event can have incredible strategic implications.

The general themes and messages provided by Central Command (CENTCOM), the International Security and Assistance Force (ISAF), and North Atlantic Treaty Organization (NATO), do not constitute strategic or operational level guidance outlining a proactive approach to SC in the Afghan Theater.[4] This paper provides a recommendation for a SC model for future operational level headquarters as they enter into a COIN environment.

Key Definitions

The United States Government (USG) uses SC to provide top-down guidance relative to using the informational instrument of national power in specific situations. It is defined as:

> *The focused USG processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advancing national interests and objectives through the use of coordinated information, themes, messages, and products synchronized with the actions of all instruments of national power.*[5]

The primary military activities that support SC themes and messages are information operations (IO), public affairs (PA), and defense support to public diplomacy (DSPD). Joint Pub 3-13, *Information Operations,* defines IO as:

> *The integrated employment of the core capabilities of electronic warfare, computer networks operations, psychological operations, military deception, and operations security in concert with specified supporting and related*

> *capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.*[6]

Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms,* defines PA as "those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense (DOD)."[7] The same document defines DSPD as "those activities and measures taken by DOD components to support and facilitate USG public diplomacy efforts."[8]

Operationalizing Strategic Communication

SC employed at the operational level in COIN is designed to effect the perceptions, attitudes and beliefs of target audiences in support of USG objectives. Effectively employing the communications means listed in the previous paragraph is important in achieving the desired information effects. But actions speak louder than words. What a military unit does also sends a SC message, and arguably this is the message that the target populations receives most effectively. Military commanders must be cognizant of this and what must be anticipated and incorporated in the overall plan.[9]

This makes SC an offensive resource and much more than just individual stories and interviews to be placed in different media venues as a result of an event. SC is comprised by everything, kinetic and non-kinetic, that is done on the battlefield and throughout the Area of Operation (AO) and Area of Interest (AI) to achieve an information effect.

As a principle of war, the term offensive is synonymous with initiative. The surest way to accomplish an assigned mission is to gain and exploit the initiative and to force an enemy to react in a desired and anticipated manner. Military commanders desire the initiative to control their environment and impose their will on the enemy.[10] By employing SC as an offensive resource it is operationalized and more effectively synchronized in operational plans (OPLANs). The operationalization of SC will establish an offensive, aggressive approach in the employment of this essential line of operation (LOO) in the COIN fight. The center of gravity (COG) for both the insurgent and

counterinsurgent at the operational and tactical level is the population. The first step to gaining the initiative from the insurgent is to understand how they are communicating their messages to the people and what the effectiveness of that message is. With that knowledge the counterinsurgent can then formulate a plan that will force the insurgent to react to the environmental and information effects created by an offensive, aggressive SC strategy. While this will be a challenge because it is impossible to control the information environment 100% of the time, maintaining the flexibility to react rapidly and truthfully to unpredictable events can undermine the insurgent's message.

In order to effectively accomplish this concept, SC should be prioritized as a LOO on equal footing in the COIN spectrum with security, governance, and development, ensuring continuous strategic, operational, and tactical leadership attention and input across the information environment. The steps in developing this offensive model can be identified by answering the "five W's" (why, who, where, what, when), and most importantly the "how" of the counterinsurgent strategic communication environment.

The first step is answering the "why." This will identify what information effect we wish to achieve in the macro as well as with each target audience. Step two is "who and where." Who are the target audiences that the counterinsurgent is trying to reach and where do they reside? There are risks of unintended negative second and third order information effects when delivering an effective message to the desired target audience. The key to this step is how to effectively synergize or mitigate that risk in the information environment. Step three is "what." What are the messages that we want to be accepted by each target audience? Step four is the "when." When do we send the messages and at what are the frequency of the messages to specific target audiences. Finally, the "how" is the most important, and it is two-fold. How do we deliver the messages? What is the best vehicle for delivery to the desired target audiences? A message can be delivered kinetically or non-kinetically, by action or deed, through the media or through interpersonal communication that can achieve the desired effect at the tactical, operational, or strategic level individually, sequentially, or simultaneously. Additionally, when delivering the message by interpersonal means the U.S. messenger may

not be the most effective. Instead key influencers within the cultural milieu of the target audience (TA) could act as a principle agent to achieve the best information effects. The second "how" is the most difficult. How do we measure the effectiveness of the message within each target audience?

Why Strategic Communication Needs to be a Separate Line of Operation

The USG instruments of national power are expressed in the acronym DIME standing for diplomatic, information, military, and economic elements. Diplomacy is the principal instrument for engaging with other states and foreign groups to advance U.S. values, interests, and objectives. The informational instrument is diverse and purposely has no single center of control. As part of the U.S. Constitution and the right to freedom of speech, information is freely exchanged with minimal government control. Information available from multiple sources influences domestic and foreign audiences including citizens, adversaries, and governments. The USG uses SC to provide top-down guidance and focus in specific situations for specific themes and messages. The purpose of the military instrument of national power is to fight and win the nations wars. The economic instrument is the free market economy itself. In keeping with U.S. values and constitutional imperatives, individuals and entities have freedom of action worldwide. The USG's financial strategies and resources support the economic instrument of national power.[11]

There is a clear parallel between our instruments of national power and the traditional COIN LOOs. Joint Publication 1-02 defines a LOO as "a logical line that connects actions on nodes and/or decisive points related in time and purpose with an objective."[12] LOOs are used for synchronizing operations against enemies that hide among the populace. A plan based on LOOs coordinates the actions of joint, interagency, multinational, and host nation (HN) forces toward a common purpose. Each LOO represents a methodology along which the HN government and COIN force commander intend to counter and gain the initiative over the insurgent strategy. The desired end state is the acceptance by the people of the legitimacy of the HN government.[13]

Field Manuel (FM) 3-24, *Counterinsurgency*, lists examples of COIN LOOs as: Combat Operations/Civil Security Operations, HN Security Forces, Essential Services, Governance, and Economic Development.[14] The FM uses the figure below to represent the individual LOOs as a single strand of rope. Once intertwined the rope becomes stronger than the individual strands. "The overall COIN effort is further strengthened through IO, which support and enhance operations along all LOOs by highlighting the successes along each one."[15]

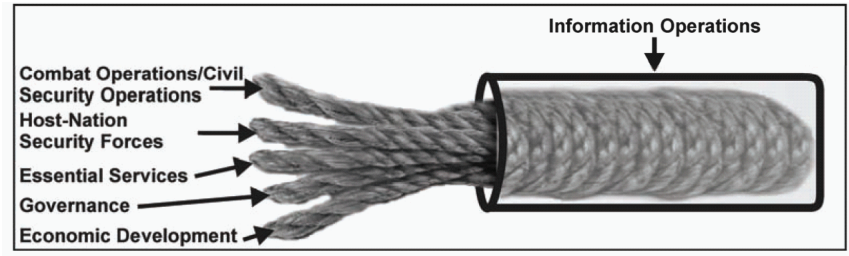

Figure 1: The strengthening effect of interrelated logical lines of operations[16]

Combined Joint Task Force (CJTF)-82 used the same approach as depicted in FM 3-24 as it developed LOOs for Operation Enduring Freedom (OEF) VIII replacing IO for SC in order to better incorporate all informational capabilities and resources available to an operational level headquarters. As the headquarters prepared for the Mission Readiness Exercise a specific decision was made not to place SC as a separate LOO because it was felt that SC was an essential part of each of the identified LOOs: security, governance and development – exactly as depicted in figure 1. In retrospect, there was an inherent flaw in this logic. Once CJTF-82 deployed, the operational level plan was assessed and evaluated on a monthly basis. Objective and subjective metrics of the commander's vision of the desired end state of each LOO were reviewed with the task force leadership at monthly Commander's Operational Assessment Briefing (COAB). Unfortunately, even though it was a function of security, development and governance, there was no specific evaluation criteria associated with SC. Consequently SC was not synchronized and coordinated across the LOOs with a specific objective, but rather addressed in each LOO individually. The outcome was a SC plan that was not as effective as it could have been. It did not have an overarching plan focusing efforts at the desired target audiences

(people, military, and government) that quickly exploited the successes of the Afghan people and government while also uncovering the brutal tactics of the enemy in their war against people of Afghanistan. What was missing by not having SC as a separate LOO was a vision from the commander of what the informational end state should be.

The key to an offensive information environment lies in clearly stated information intent. Subordinate commanders need a vision of what the commander wants the information environment to look like at the end of the military operation. This articulates what the desired perceptions and attitudes of the TAs are, and what are the information capabilities of the enemy at the conclusion of the operation.[17]

In *On War*, Carl von Clausewitz famously identifies a trinity of the people, the military, and the government. Clausewitz argued that the active support of each segment was critical to success.[18] This trinity remains as relevant in the COIN struggle today as ever. In American society, and arguably every society in this information age of a 24/7 news cycle, the media plays a unique and important role by serving as the critical information link among the three elements.[19] The effective conduct of military operations demands effective communication with the people. Successful SC is the ability to exploit the information link.

Security, governance, and development mirror the instruments of national power of military, diplomacy and economics. The missing LOO is SC to mirror information. Using SC as an offensive tool places it as a separate LOO on equal footing in the COIN construct as security, governance and development. It would require a desired end state articulated by the commander and objective and subjective measures of effectiveness (MOE) as well as measures of performance (MOP) to assess its progress and effectiveness in the same manner as the other LOOs.

How the Insurgent Employs Strategic Communication

If resistance is equal to means times will[20] – the ability of the insurgent to maintain their fight against the HN is in direct relation to the will of the people to provide active or passive support. SC influences the will of the people and their perception of how the HN government and

the coalition forces that are supporting them can provide for the needs of the people. Insurgents use SC to affect perceptions, attitudes, and beliefs as well. These perceptions become reality and, as was described in Clausewitz's trinity, is the bond that either unites the people to the government, or to the insurgent.

Yet the insurgent's SC has no responsibility to be truthful and freely exaggerates or lies to ensure his message is delivered. He is not obliged to prove; he is judged by what he promises, not by what he delivers. The new media of the information age also aid this effort. The enemy can transmit a message in real time bypassing editors and restrictive source requirements. Consequently, propaganda is a powerful weapon for the insurgent. With no real or positive policy but with good propaganda, he can win.[21]

The highly respected British strategist Colin S. Gray wrote an interesting essay in 2005 offering 12 specific characteristics that can be used as an example of how the world views the American way of war. These include: Apolitical, Astrategic, Ahistorical, Problem-Solving Optimistic, Culturally Ignorant, Technologically Dependent, Firepower Focused, Large-Scale, Profoundly Regular, Impatient, Logistically Excellent, and Sensitivity to Casualties.[22] Gray's thesis of these characteristics is credible because he is not a U.S. citizen. His view therefore, allows an outside perspective on how we fight and the distinctiveness that separates us from rest of the world. Though each of these characteristics can arguably be explored within the COIN environment, it is worth focusing on some in order to better understand how the enemy could be using these perceptions against us in their effective use of SC.

Culturally Ignorant:

> *Americans are not inclined to be respectful of the beliefs, habits, and behaviors of other cultures…the American way of war have suffered from the self-inflicted damage caused by a failure to understand the enemy of the day.*[23]

Of course, this does not only apply to the enemy, but to the population where we are fighting COIN. The enemy SC will exploit every opportunity where coalition forces violate cultural traditions or norms

to exasperate local or Muslim people emotions with the intent of inflaming the local populace or international community against our operations.

Technologically Dependent:

> *America is the land of technological marvels and of extraordinary technology dependency…American soldiers say that the human beings matter most, but in practice the American way of war, past, present, and prospectively future, is quintessentially and uniquely technologically dependent.*[24]

The enemy's SC exploits these both defensively and offensively. As an example from the defensive perspective the enemy exploits every opportunity to portray our use of Unmanned Ariel Vehicles (UAVs), or drones, in the media as a robotic U.S. instrument of death that is employed due to our lack of personnel on the ground and that they arbitrarily kill innocents with their Hellfire missiles. In fact the UAV was developed, and is primarily used as a reconnaissance asset. Their onboard cameras stream back real time video and provide commanders at all levels a perspective that cannot be seen by the units on the ground. They are armed and have the technology to deliver precision guided munitions, but their employment in that function is less than desired and in the event close air support is required other platforms available produce far better effects than the UAV.

The insurgent has used this dependency as an offensive tool as well. The monopoly enjoyed by nation-states over information as an element of power was lost as technology improved and as the means to transmit information became smaller, faster, and cheaper.[25] The information explosion of the last decade has produced a wave of new media vehicles that the insurgent is effectively employing against the U.S. and its coalition partners. Islamic extremist websites grew from twenty to over 4,000 in only five years.[26] Individuals and non-state entities, armed with new media capabilities and unfettered by bureaucratic, moral, or ethical standards will continue to use information as an asymmetrical weapon.[27] The paradox of this technology is that we refuse to exploit the capability ourselves and yield instantaneous information effects to our enemies.

Firepower Focused:

> *It has long been the American way in warfare to send metal in harm's way in place of vulnerable flesh....Needless to say, perhaps, a devotion to firepower, while highly desirable in itself, cannot help but encourage the U.S. armed forces to rely on it even when other modes of military behavior would be more suitable. In irregular conflicts in particular…resorting to firepower solutions readily becomes self-defeating.*[28]

Our enemy's use this "David and Goliath" analogy of firepower and proportionality with great effect. Typically, when close air support is used in a contact with coalition troops and insurgents in Afghanistan, there is a claim of non-combatant casualties by the insurgent. The mere claim is enough to garner international attention in the media. Compounded with the speed by which the insurgent posts these accusations the information effect is significant. Islamic radicals and other factions opposed to the United States have demonstrated no respect for the truth when they manufacture charges of American atrocities. While the U.S. forces take great care to avoid inflicting civilian casualties, such casualties will inevitably occur. A few injured civilians become a massacre of innocents, first in the Arab press and then often substantiated by the Western media.[29]

Regardless of the accusations being proven false or not, the effect is achieved and the perceived civilian casualty death toll continues to climb. The media victory is won both at the local population target market as well as with the populations of the United States and our coalition allies. In today's information environment once the message is delivered to attempt to deny or counter it becomes largely ineffective.[30]

Profoundly Regular:

> *Few, if any, armies have been equally competent in the conduct of regular and irregular warfare….As institutions, however, the U.S. armed forces have not been friendly either to irregular warfare or to those in its ranks who were world-be practitioners and advocates of what was regarded as the sideshow of insurgency. American soldiers…have always been prepared nearly exclusively for real war, which is to say combat against a tolerably symmetrical, regular enemy.*[31]

Gray's assessment gains credence as one examines the lack of new doctrine concerning counterinsurgency in the period immediately following the Vietnam War. The U.S. Army failed to form a consensus on the lessons of Vietnam and did not accept the idea that revolutionary war requires a qualitatively different response from the conventional warfare it knows so well how to fight.[32] Our inability to initially recognize or acknowledge that our forces were involved in insurgencies in both Iraq and Afghanistan is another example of our reticence as an army to engage in this type of warfare. Our enemies know this and use it to their benefit. Since the insurgent alone can initiate the conflict, strategic, operational, and tactical initiative is his by definition. He is free to choose his hour and to wait safely for a favorable situation.[33] An Army fighting conventional warfare tactics cannot defend adequately these asymmetric tactics. Only since new counterinsurgency doctrine was published in 2006 have we seen real progress in Iraq.

Afghanistan continues to be a challenge. New COIN doctrine is being implemented to include an understanding of the importance of SC. However, the lack of security forces (both Afghan and coalition) serving throughout the country to ensure the perception of safety to the Afghan population is working against HN and coalition forces. The enemy will continue to use their SC and their perception of our desire to fight a conventional fight against us as U.S. forces work to convince the Afghan people, as well as international and domestic TA's of our well meaning intensions.

Impatient:

> *Americans have approached warfare as a regrettable occasional evil that has to be concluded as decisively and rapidly as possible.*[34]

The American characteristic of impatience is a result of our economic and political systems. The United States is a nation of people who expect immediate satisfaction and our enemies use this against us. While both the insurgent and counterinsurgent are vying for the support of the people, so are they vying for the attention of the U.S. population. A target audience of enemy SC is the will of American people. They perceive this to be our strategic and operational COG. As evident in the Vietnam War, the American people dislike a protracted insurgency

regardless of battlefield victories. Using this example as an historic defeat of the U.S. military, all the modern day insurgent has to do is survive. Winning simply means not losing. Knowing the impatience of the U.S. population time is on the side of the insurgent.

Sensitivity to Casualties:

> *In common with the Roman Empire, the American guardian of world order is much averse to suffering a high rate of military casualties….Both superstates had and have armies that are small, too small in the opinion of many, relative to their responsibilities. Moreover, well-trained professional soldiers, volunteers all, are expensive to raise, train, and retrain, and are difficult to replace. American society has become so sensitive to casualties that the domestic context for U.S. military action is no longer tolerant of bloody adventures in muscular imperial governance.*[35]

October 3, 1993 is a red letter day for the enemies of the United States. The impact of, and eventual reaction to, the loss of eighteen special operations and conventional U.S. military men on that day in Mogadishu, Somalia, has become an essential text book tactic in the strategic kitbag of our enemies. Our enemies continue to seek a similar spectacular catastrophic event for its informational effect. Though American deaths are the most effective, massive HN civilian casualties will also degrade U.S. support of a counterinsurgency.

In addition to the mass casualties, inflicting one or two deaths a day, every day, with IEDs has the same informational effect over time. Coupled with graphic video, the act and images create a powerful negative effect on the American people.

It is safe to say that the insurgents and international terrorists in Afghanistan are using these perceptions of how Americans fight their wars against us in their SC not only to the Afghan people, but also to the international community and the U.S. population. One does not have to agree 100% with Mr. Gray to see the value of his observations. As part of a strategic intelligence preparation of the information environment, understanding how the United States is perceived by others and how the enemy may use those perceptions against us in

their SC, an operational headquarters can anticipate information opportunities and positively influence an offensive SC plan.

Desired Effects and Objectives for Strategic Communication

The idea that an insurgency wins or loses by its ability to win the hearts and minds of the people is an old cliché. However, like so many clichés, it happens to be true. While some insurgencies might be defeated by sheer brute force, this option is ruled out by any Western democracy today on the grounds of morality and practicality. Additionally, brute force typically only grows more insurgents. Maintaining American legitimacy while waging a COIN war, as viewed in the eyes of the world and the eyes of the U.S. people, requires that we adhere to the high standards of behavior demanded in the Western democratic tradition. It also is critical to help allied governments fighting insurgents to win the active, or passive, support of their populations.

In September 2007 the DOD published an SC plan for Afghanistan. Within this document it outlined the desired endstate for the SC as "The Afghan people and people in Allied and partner countries recognize and support the efforts of the Afghan government, the United States, its Allies and partners in stabilizing and reconstructing Afghanistan. The Afghan people strongly support their government and reject insurgency, terrorism, and the narcotics trade."[36] Though published by DOD and intended at the strategic level, this endstate addresses the strategic, operational, and tactical levels. While the Brigade Combat Team (BCT) commanders are working directly with the population and the Afghan leadership and security forces at the provincial levels, they also have direct and continuous contact with media from both the United States and international press. Clearly, tactical events and actions have both operational and strategic impacts.

At the operational level CJTF-82 identified an overarching COIN approach that focused on the people of Afghanistan and sought to achieve effects in concert with the DOD plan. These effects addressed both the Afghan people as well as the insurgents. For the Afghan people those effects are: Connect People to the Government, Build Trust and Confidence in Government, and Solidify Popular Support of Government. The SC effects on the insurgents are: Separate Insurgents

from the People, Limit Insurgent Options to Reconcile, Capture, Kill, or Flee, and Discredit Insurgent Vision and Ideology. This COIN approach is depicted in the following slide that was used in the CJTF-82 command brief given to VIPs visiting the headquarters at Bagram Airfield near the capital Kabul, Afghanistan.

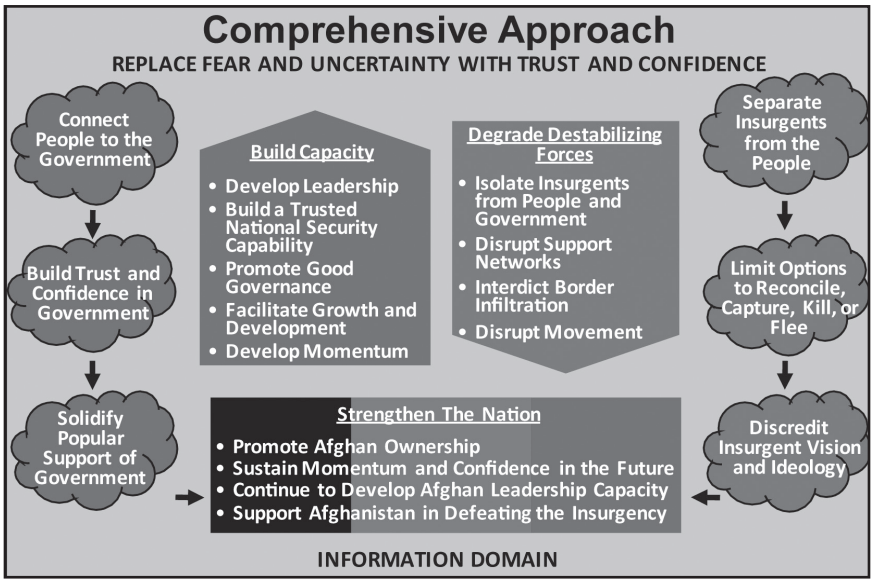

Figure 2: Comprehensive Approach[37]

In COIN the focus is more on discrediting the insurgent's SC and means in the eyes of the population than on taking out the insurgent kinetically. Insurgents are often the brothers and cousins of the population you are trying to influence. Killing or capturing them will not win hearts and minds, but may well fuel future recruits. The "win" must be based on convincing the people (and the insurgents where possible) the legitimacy of the HN government, and that their way has the best interests of the population at heart, which also means that the insurgent's message and methods are discredited.[38]

Identifying Target Audiences

The DoD SC Plan for Afghanistan identifies twelve target audiences (TA) at the strategic level. Those TAs are: The Afghan Population, the Afghan Government, the Government and Military of Pakistan, the Pakistan Population, Governments of ISAF Troop Contributing

Nations, Populations of ISAF Troop Contributing Nations, Enemy Leadership, Taliban Rank and File, Governments of Central Asia, Central Asian Populations, International Government Organizations (IGO) and Non-Governmental Organizations (NGO) Community, and finally U.S. domestic audiences.[39]

While these TAs are focused at the strategic level, from an operational perspective this list is too broad. As discussed throughout this document, the primary target audience and COG in any insurgency/COIN is the people. In addition to the Afghan people, both the Afghan leadership and security forces are critical to the success in the COIN efforts and are operational level TAs. Second only to the Afghan TAs are the U.S. TAs. Operational SC can and should be directed at the U.S. policy makers as well as the U.S. population since the goal of SC is to inform and educate. ISAF contributing government leadership and populations are also critical TAs and can be effectively reached at the operational level. The final TA that can be effectively reached at the operational level is the international Muslim community.

Themes, Messages and Talking Points

Themes, messages and talking points are key elements of SC and are nested horizontally and vertically and anchored in truth. A theme is a topic of discourse or discussion that is used by strategic communicators and directed to a TA in order for them to understand and accept an idea or concept. An example of a theme for Afghanistan could be "the Taliban are a negative force that purposely targets innocent Afghan civilians. They engage in criminal activity and brutal tactics for their own gain and cannot offer long-term solutions for the people of Afghanistan."

A message is nested under a theme and is more specific in supporting information. Messages are directed to specific TAs. Strategic communicators deliver the message that will resonate the most effectively. Different messages directed at different TAs can support the same theme. As an example, the following message supports the example of the theme proposed in the previous paragraph. "The Taliban seek to undermine the authority of the legitimate Afghan government. Their

campaign of terror is designed to convince the people of Afghanistan that their government cannot provide security."

Talking points are timely and truthful anecdotes specific to the message being delivered and support one of the themes. Just as there are numerous messages per theme, there can be numerous talking points per message.

The Public Affairs officer for an organization is responsible to provide the themes and messages provided from the higher headquarters and pertinent talking points to the leadership and strategic communicators. What they will not do is make a decision regarding how often messages should be delivered to the TAs. This is a leader decision. What TAs are addressed, how often they are addressed, and the frequency of the messages should be planned in advance as part of an offensive SC plan nested in the overall campaign. Critical to the success of an offensive SC plan is the consistency of themes and messages. Messages delivered to TAs should be consistent and frequent. Measureable objectives should be established as part of the SC LOO with measures of effectiveness (MOE) identified for those objectives. MOE must be part of initial planning such that a baseline can be established against which to measure. A key function of the MOE will be to determine if the frequency of messaging is adequate; whether or not the message is resonating with the TA. One MOE for determining whether a message is resonating with a TA is if the message is repeated or supported by that TA. Determining the correct frequency of messages delivered to the correct TA, and incorporating that as a pillar of the operation is the goal of a proactive, offensive SC plan. This defines the operationalization of SC. How SC is synchronized within the campaign ensures the seamless application of this LOO.

Synchronizing SC with the other LOOs – The Joint Effects Process

The synchronization of SC with all the kinetic and non-kinetic resources and assets across a combined-joint task force is daunting challenge and can only accomplished by the direct involvement and monitoring of the top leadership and staff of an organization. In order to synchronize SC it must be planned in advance and in concert with the other LOOs. This Joint Effects Process (JEP) is done at the operational staff level

under the direct supervision and guidance of the commander and his key subordinates (deputy commander, chief of staff, director of operations).

The operational level staff of CJTF-82 during OEF VIII had a series of boards, bureaus and cells, developed into a battle rhythm, which culminates in a monthly Commanders Operational Assessment Brief (COAB) delivered by the CJTF staff and BCT commanders to the CJTF-82 Commanding General (CG). These boards, bureaus and cells (BB&C) all had their own specific designated outputs that fed linearly and sequentially to the next BB&C. The JEP is based on the standard targeting methodology of decide, detect, deliver and assess (D3A). This is both a lethal and non-lethal targeting process that supports the LOOs, their objectives and the desired effects as the basis for planning and recommendations to sustain, alter, or change planned operations or events.

Objectives are defined as "the clearly defined, decisive, and attainable goal toward which every operation is directed."[40] Objectives prescribe friendly goals. Effects are "the physical or behavioral state of a system that results from an action, a set of actions, or another effect."[41] Effects describe system behavior in the operational environment. MOE are "a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect."[42] They are the basis of evaluating an effect. They answer the question "Is the force doing the right things, or are additional or alternative actions required?"

The JEP as articulated in D3A starts with the "decide." Decide answers the question what can we do to achieve the desired objectives and effects with each of the LOOs? Detect identifies where we achieve the effects for maximum results. Deliver identifies who or what delivers the action that achieves the desired effect. Assess at the operational level is done at the CJ5 (Future Plans) staff section using regularly scheduled, reoccurring polling of TAs, as well as by input from the separate staff sections at the CJTF headquarters, and by getting direct feedback by the BCT commanders. The assessment is done not only for the SC LOO, but also for security, governance and development.

The JEP is conducted throughout the CJTF battle rhythm and ensures a methodical, thorough, synchronized and comprehensive method to analyze, measure, and maintain the initiative in an offensive approach across all LOOs at the operational level of COIN. From the SC standpoint, the JEP confirms or denies the frequency and effectiveness of the information engagements, planned, or unplanned, across the information environment. With that analysis and recommendations from the staff, the CG or his designee, can make the decision to increase or decrease frequency, methods or messages to each TA.

Framing a Comprehensive, Offensive SC Model

As previously stated, the CJTF reoccurring battle rhythm meetings culminates in a monthly Commanders Operational Assessment Briefing (COAB) delivered by the CJTF staff and BCT commanders to the CJTF-82 CG. The purpose of the briefing is to provide an assessment of the operational environment to the CG. Each LOO is assessed based on objectives and desired effects at the operational level, by the CJTF staff, and at the tactical level by the BCT commanders. At the end of the briefing the CG gives guidance to commanders and staff focusing on the LOOs and their respective objectives and effects. The chart used to visualize this is called the Effects Hierarchy. The guidance given provides the staff and subordinate commanders a baseline from which to work from and commanders intent through the next COAB.

The effects hierarchy becomes the visual aid that assists in the synchronization of all the LOOs toward the COIN goals articulated in the Comprehensive Approach (see figure 2.). It is the base plan for the model and ensures proactive analysis and initiative is applied to achieve the objectives.

As stated previously, SC was not identified as a separate LOO during OEF VIII, but was rather considered embedded in each of the other three LOOs. Unfortunately, by not identifying SC as a separate LOO there were no objectives or MOE established for SC and there was no systematic, reoccurring, objective method of evaluating the information effects.

Specific objectives and effects for SC within the effects hierarchy should be determined in relation to the situation and assessment

of the current environment. SC objectives should be based on the number of information engagements in relation to specific TAs and the other LOOs. Desired effects for these objectives should focus on the understanding and acceptance of the messages by the specific TAs. There are multiple methods of measuring the effectiveness of the information engagements. The most objective method of knowing when you have achieved your desired effects is when your TA repeats or supports by action, word or deed, your messages. This can be determined by polling results of the population, local, international, or national (U.S.) media or news stories, quotes from key local, national, or international leaders, and the objective observations or subjective perceptions of the BCT commanders. All of these information effects and results are analyzed and presented to the CG during the COAB.

Additionally, systems need to be in place to provide a real time informational response to the events that will occur on a daily basis either through planned or unplanned operations and actions in order to gain and maintain the informational initiative on the enemy. Everything we do and everything the enemy does have an information effect. The positive is exploited at the informational level to ensure the desired effect is achieved with the TA. The same should be done to exploit the negative enemy actions as well. These types of events become information decision points and a battle drill takes place at the headquarters in the Joint Operations Center (JOC) to quickly exploit the event and provide an offensive information engagement to desired TAs.

This is accomplished by manning an information cell comprised of public affairs and information operations representatives on the JOC floor continuously operating in the vicinity of the Chief of Current Operations, who is responsible for the day to day operations in the JOC. The information cell will provide "information ammunition" for distribution to the desired TAs in the form of an information engagement. The leadership of the CJTF must trust the judgment and capabilities of the information cell in order for this technique to be successful. This reinforces the requirement for the CJTF commander to articulate exactly what his vision is for the information end state. Using that commander's intent the information cell can act quickly

and decisively in order to exploit an information opportunity. The Chief of Current Operations, or at most the Director of Operations (CJ3), must have release authority for these information engagements.

Another responsibility of the information cell would be to manage the Commanders Web Page. This is an unclassified web page which provides a daily update of current written and visual information, accessed from internet by anyone with a computer. The Commander's Web Page uses the internet to deliver to the desired TA's a current, up to date information engagement that utilizes real time talking points to constantly reinforce the operational level themes and messages.

Unplanned or unintended negative actions by friendly forces, also known as "wild cards," must also be acted upon immediately. The enemy will most certainly exploit this. Speed is critical here as well and involves both the leadership and the staff. Press releases, press conferences, interviews, phone calls to key host nation leadership and influencers, etc., takes place as quickly as possible in order to ensure this negative event is announced first by the HN or by the Coalition Forces, and not the enemy. An explanation is given and assurance that a combined investigation is being done. This counters the sensationalism of the informational effect that the insurgent will surely attempt to convey.

The enemy has also exploited claims of non-combatant casualties following engagements where close air support (CAS) were used in support of coalition operations. Every air craft has cameras on board that record their engagements. A simple solution is to immediately release this footage which shows rifle or RPG fire coming from the house that was engaged. Unfortunately, the ability to declassify and release this type of footage to the media has been extremely bureaucratic and time consuming. By the time the release authority has been given a week has passed and the negative event has become a fact in the minds of the TA regardless of proving it false or not. Some headway has been made to improve the process, but the true fix is having the release authority at the CJTF CG level. Only by having the release authority at the operational level commander can we effectively achieve the speed to counter the enemy's disinformation capability.

Conclusion

One can look in any nationally circulated periodical, surf the internet, or flip through cable television on any given day and see an example of an unintended, or poorly articulated SC message, whether diplomatic, military or economic. Within this information spectrum, there are multiple stories of Afghanistan and the counterinsurgency struggle that the country is involved in every day. Operational level headquarters cannot be passive or reactive in how they function in the information environment unless they are willing to accept defeat. SC is a LOO that is critical in this political and physical struggle. The JEP creates an offensive model that, when employed effectively, provides a proactive methodology that can anticipate information opportunities and maintain the initiative over our adversaries. The messages of the Afghan government and coalition forces need to be presented in a positive, truthful, and proactive manner to ensure the support of the Afghan people and the international community in a struggle with global implications.


Prudens
Futuri

Empowering United States Public Diplomacy for the War of Ideas

Lieutenant Colonel Douglas W. Little
United States Army National Guard

Following the events of September 11, 2001 (9/11), President Bush described the Global War on Terror (GWOT) as more than a battle of arms, but a battle of ideas.[1] In his 2002 National Security Strategy (NSS), President Bush placed particular emphasis on implementing effective public diplomacy as a means to gain the trust and confidence of those who may otherwise support international terrorism.[2] President Bush hoped to capitalize on public diplomacy's powerful ability to foster relationships and cultural understanding among people of differing nations to influence global attitudes and actions in the war of ideas.[3] However, eight years into the GWOT, international polling data demonstrates U.S. failure to gain substantive ground in the war of ideas.[4] In fact, years of marginalizing public diplomacy has left the United States with an emaciated and arguably ineffective weapon in the war of ideas.[5] Enveloped within the Department of State (DoS), devoid of an independent vision, and a shadow of its prior budgetary and personnel strength, current U.S. public diplomacy remains ill-prepared to confront the crucial and formidable struggle in the battle of ideas now or in the foreseeable future.

This paper explores how U.S. hubris regarding its global influence in a unipolar world led to marginalizing the once independent and effective public diplomacy effort under the United States Information Agency (USIA). Additionally, a presupposed universality of the democratic peace theory and a fundamental misunderstanding of the roots of international terrorism continue to obscure a definitive strategy and progress by U.S. public diplomacy in the war of ideas. The paper concludes with recommendations to empower U.S. public diplomacy and establish a sustainable and effective vision for confronting the war of ideas in the future.

Public Diplomacy Failure Analysis

"If I were grading, I would say we probably deserve a 'D' or a 'D-plus.'"[6] Stark testimony from former Defense Secretary Rumsfled, delivered to the U.S. Army War College in March 2006, regarding U.S. performance in the war of ideas to date. Such assessment is considerably more damming when conceding, in addition to the President's 2002 NSS, the *United States National Strategy for Combating Terrorism* also concluded success in the GWOT hinges on winning the war of ideas.[7]

Considering America's war of ideas began long before the events of 9/11, Secretary Rumsfeld's current assessment of U.S. strategy in this struggle is rather generous. Reasonable arguments might trace the West's war of ideas with Islamic extremism as far back as the fall of the Ottoman Empire or earlier.[8] However, America's war of ideas ostensibly began with the Iran Hostage Crisis. Analyzing this crisis, International Relations Professor, Adda Bozeman, in 1979 described America's ongoing intelligence collection failures and profound ignorance of complex cultural patterns and historical perspectives of the region as the sources of that crisis.[9] These criticisms appropriately reverberate in today's GWOT (now Overseas Contingency Operations) and painfully illustrate just how little progress the United States has made over the last 30 years in the war of ideas.

Such lack of progress in the war of ideas warrants strategic reevaluation. Developing an effective and enduring strategy for U.S. public diplomacy in the war of ideas requires analysis of factors contributing to America's ineffective response to its greatest security challenge in decades. While a multiplicity of factors undoubtedly contributes to U.S. public diplomacy's recent ineffectiveness, the most prominent impediments are: America's power paradox, inappropriately applying a 'one size fits all' universality to the democratic peace theory, and America's fundamental aversion of religious ideological struggles.[10]

America's Power Paradox – The Dismantling of United States Public Diplomacy[11]

The fall of Communism in the early 1990's placed America in a position of unparalleled dominance. As the world's preeminent

superpower, Congress argued democracy's triumph over Communism would itself suffice as the most effective and lasting public diplomacy for the United States.[12] Competition over scarce budget dollars pressed Washington to question the continued need for a broad, independent public diplomacy agency in a unipolar world.

Following a decade of progressive budget cuts and staff reductions, a major restructuring of U.S. public diplomacy dramatically reduced its autonomy and flexibility.[13] In October 1999, the Foreign Affairs Reform and Restructuring Act reduced U.S. public diplomacy to a subsidiary within the DoS. The Act placed U.S. public diplomacy under the direction of a new Under Secretary for Public Diplomacy and Public Affairs.[14] The fledgling Department of Public Diplomacy and Public Affairs, as America's premier weapon in the war of ideas, found itself ill-suited to meet the needs of an aggressive foreign policy agenda by the Bush administration. In the absence of an established, effective, and robust public diplomacy effort to help successfully facilitate this new foreign policy, the stage was set for a dismal collapse.

In the GWOT, the Bush administration needed a well-orchestrated public diplomacy effort to reassure the international community that the objective was not U.S. imperialism or a threat against Islam, but a global struggle against those who perpetrate terrorism. Unfortunately, due to the organizational structure within the State Department, the Under Secretary of Public Diplomacy and Public Affairs lacked direct oversight or control of the regional bureaus and field posts needed to synchronize the agenda.[15] To compound the problem, regional field posts lacked a coordinated strategic approach to their mission.[16] Some field posts were left vacant. Moreover, of those filled, only 60% contained officers with the minimum required language proficiency skills.[17] Security concerns limited the effective outreach of these posts and average staff tours in the Middle East region were 22% shorter than tours in other parts of the world.[18]

Maintaining a forward posture, President Bush used his 2002 NSS to declare the United States would act preemptively and unilaterally, if necessary, to prevent future hostilities against American interests.[19] While this stance was a domestic public affairs success, without the necessary foundation established by an effective public diplomacy

agency, such an aggressive approach quickly created concerns of U.S. hegemony within the international community.[20] These perceptions undermined American influence abroad and eroded much of the world's sympathy and support previously garnered after events of 9/11.[21] As President Bush worked to build a case against Iraq and formulate a coalition, Pew Research Center polls indicated that U.S. public diplomacy failed to contain growing animosity toward U.S. foreign policy across the globe.[22] World public opinion trends from 1999 to 2003 demonstrated marked decreases in U.S. favorability ratings in both Muslim and European countries.[23]

On May 1, 2003, after approximately two and a half months of conflict, the President stood aboard the USS Abraham Lincoln in front of a banner that proclaimed "Mission Accomplished" to announce that major combat operations in Iraq had ended.[24] What had only begun was the devastating blow to U.S. public diplomacy that would degrade its ability to influence world opinion on U.S. foreign policy. In the subsequent months, extensive investigations failed to uncover substantial or conclusive evidence to support the claims by U.S. intelligence agencies that Saddam Hussein possessed weapons of mass destruction or had definitive ties to al-Qaeda.[25] Consequently, America's moral authority was severely marred, debilitating its soft power in global influence.[26] At the time, even former U.S. Under Secretary of Public Diplomacy and Public Affairs, Karen Hughes, acknowledged that repairing the U.S. image abroad could take years if not decades.[27]

One Size Does Not Fit All

The second impediment to U.S. public diplomacy's effectiveness in the war of ideas is a misunderstanding of the Muslim culture, attitudes and behaviors. In an oversimplification of the democratic peace theory, America's foreign policy objective of democratizing the Middle East neglects to consider how such an agenda may affect regional culture.

Profound respect for history and cultural tradition defines and binds Middle Eastern cultures.[28] As such, fears regarding Western colonization of their holy lands remain at the forefront of their consciousness. U.S. military stationed in the Middle East and Western coalition forces invading Iraq and Afghanistan exacerbate these concerns.[29] Similarly,

despite Western views of Saddam Hussein and the Taliban as abusive regimes, removal of these leaders overlooks that, in the Muslim faith, even corrupt or tyrannical leaders engender obedience, so long as they do not interfere with Muslim's religious practices.[30] Thus, attacks on these regimes threaten even moderate Muslims, widening the gap with the West and further complicating the war of ideas.[31]

Imposing Western values on Muslim cultures similarly complicates the war of ideas. Civil liberties, human rights, separation of church and state, and political freedoms honored in the Western democracies have no applicable translation in the Muslim culture.[32] Muslims argue, these principles fail to honor the primacy of Islam and are therefore Godless, and represent the West's attempt to corrupt Islam and suppress Muslims.[33] Attempts to demonstrate religious tolerance to the Muslim culture also fail to resonate. Muslims consider religious tolerance as evidence of moral decline rather than virtuous.[34] What the West views as freedom, Muslims view as purposeless gratification of the individual.[35] Muslims argue Islam offers personal submission to a higher authority.[36] Therefore, U.S. policies espousing the spread of democracy, promoting individual liberties or, preserving human rights will likely engender resentment, suspicion, and resistance with target audiences in the Middle East. To Muslims, such agendas suggest a Western attitude of political and moral superiority over Islam.[37]

Application of Western values to theorize the etiology of Islamic terrorism similarly obscures the true foundations of this extremism, further complicating strategic development in the war of ideas. Perceptions of social injustice, income disparity, and lack of political representation, as the causes of Islamic terrorism dominate Western political thought.[38] However, historical analysis refutes these theories as problems existing in the Muslim world throughout the modern era.[39] Rather, the intrusion of Westernization into the Muslim world likely fuels current Islamic terrorism.[40] Accelerated by globalization, Western influence directly threatens to disrupt the social fabric that dominates the Muslim world.[41] In Muslim societies, religion is organic and loyalty to the extended family within a patriarchal structure is implicit.[42] This social structure is hierarchical and everyone knows his or her place.[43] Individuality or disloyalty to this social architecture is strictly shunned,

and at times with dire consequences, as evidenced by "honor killings."[44] Thus, intrusion of Western social values threatens to dismantle Muslim social and religious structures that provide the very foundation of their societies.[45] Such perceived external threats stimulate greater religious conviction among Muslims and mobilizes resistance as an obligation to protect Islam.[46]

America's Aversion to Religious Ideological Struggles

A final impediment to the development of an effective public diplomacy strategy in the war of ideas is America's natural aversion to religious ideological struggles. Religious tolerance, separation of church and state, and freedom of speech are fundamental to American society. Thus, the concept of discrediting religious viewpoints, even those considered extreme, is hypocritical and unnatural to most Americans.[47] Non-Muslims defining Islamic extremism to Muslims presents a formidable challenge.[48] In Islam, non-Muslims have no authority to opine on matters of the internal struggle that only Muslims can wage.[49] As a result, much of U.S. public diplomacy efforts to date disproportionately focused on addressing methods to improve America's global favorability ratings.[50] Far more relevant to U.S. national security is a public diplomacy strategy that empowers moderate Muslims around the world to confront and arrest the spread of Islamic extremism.[51] While both improving America's image and undermining terrorist organizations' ability to recruit are relevant in the war of ideas, presuming one will solve the other is a flawed strategy destined for failure.[52]

The Current State of U.S. Public Diplomacy: 'Ready, Fire, Aim'

Sun Tzu stated, "…if you know the enemy and know yourself; you need not fear the results of a hundred battles."[53] Arguably, the United States has done neither in the war of ideas. As Senator John McCain notes, abolishing the USIA and subsequently marginalizing the remaining U.S. public diplomacy programs within the DoS unilaterally disarmed the United States in the war of ideas.[54]

In fact, in the years since the consolidation of the USIA into the DoS, there is no evidence that Department officials are involving public

diplomacy when considering new foreign policy initiatives.[55] The USIA was the largest public diplomacy operation of any nation ever, as well as the world's largest publisher.[56] USIA boasted a greater overseas representation than any other U.S. government agency.[57] The merger of public diplomacy within the DoS reduced the number of public diplomacy officers by half.[58] Since the merger, the number of overseas public diplomacy staff has remained essentially unchanged.[59] Similarly, U.S. public diplomacy suffered marked reductions in funding upon merging with the DoS. Although increased from its nadir in 2001, U.S. public diplomacy's funding in of just over $800 million (including broadcasting) is less than the funding it received in 1957 (in constant dollars).[60] To add perspective, public diplomacy's current funding is approximately 4% of the DoS's overall foreign affairs budget and a mere 0.6% of the DOD's budget.[61]

Not only does the DoS fail to have a recruitment program for the public diplomacy career path, but also, public diplomacy officers are conspicuously absent from the senior-most ranks of the department, demonstrating an overall lack of integration.[62] Public diplomacy officers report that they now spend the overwhelming majority of their time addressing administrative duties as opposed to their primary intended responsibility of direct contact with their target populations.[63]

An initial evaluation that public diplomacy has horribly failed in its mission to explain the United States to other nations is an oversimplification. Deeper inspection reveals the misappropriate use of public diplomacy as a modality for crisis management. Whether driven by fiscal considerations, hubris, or perhaps a combination of both, after the collapse of the Berlin Wall, the costly 'peace dividend' presumption that the United States no longer needed to devote the continued level of funding, personnel, or effort toward its public diplomacy programs prevailed within the executive and legislative branches of government.

The choice to marginalize public diplomacy initiatives precipitated a cascading decline in America's ability to maintain its global positive image. Currently, the United States lacks the solid foundation of a world well versed in the virtues, human rights, and freedoms for which America stands and espouses. There is no established base of credibility to buffer lies and misconceptions, nor a stable network of

field ambassadors groomed by years of familiarity in their host nations to stem the tide of animosity and isolate the extremists.

What remains of the once vibrant and effective USIA is an American public diplomacy that is a mere shell of its former capability. Subsumed within the DoS, U.S. public diplomacy efforts appear fixed on a public affairs-centric focus as opposed to developing an enduring strategic plan to win the war of ideas. U.S. public diplomacy leadership lacks direct supervision, control or input of their field officers. Inadequate budgets prevent modernizing to keep pace with information technology advances or filling staffing requirements causing critical vacancies in field offices. Current public diplomacy officers appear disproportionately saddled with administrative responsibilities, impeding them performing their primary function of networking with their target populations. Similarly, many public diplomacy field officers lack the necessary language skills enabling them to engage with their target audience. This is the arsenal available to the United States to confront, arguably, the greatest challenge in the history of American public diplomacy, the war of ideas.

Failure to implement effective public diplomacy in the war of ideas also yields direct consequences for the war fighter. As anti-Americanism rises, losing ground in the war of ideas translates into greater resistance and hostility of the host populous against the deployed troops. Expanding war efforts means more frequent and perhaps longer deployments. Secondary effects adversely influence divorce rates, mental health, and retention among military members.[64]

Failure to contain the spread of extremism will produce additional regions of global hostility, requiring new mobilization requirements for military members. Similarly, failure to succeed in the war of ideas risks extending the sanctuary, funding, and recruitment of enemy forces in the GWOT.[65] A losing effort in the war of ideas may affect U.S. ability to form or maintain coalitions in the GWOT, forcing the U.S. military to assume a larger role creating more frequent and or longer deployments with larger areas of responsibility.[66] Allies may refuse to assist in the war effort, as was the case with Turkey, creating greater logistic challenges for troop, supply, and equipment movements.[67]

Inability to inspire like-minded alliances, partnerships, and coalitions to sacrifice for common interests, changes the dynamic of the operational environment for Joint Force Commanders.[68] Ability to form alliances obviates U.S. troops from shouldering far greater theater responsibilities, and averts the politically disastrous impression of American unilateralism to forward its own interests. Failure to staff the necessary number of overseas public diplomacy officers risks causing military mission drift. Military members may find themselves assuming public diplomacy roles and responsibilities that U.S. public diplomacy is understaffed and under-funded to execute.[69]

Recommendations to Empower U.S. Public Diplomacy

To improve the effectiveness of U.S. public diplomacy, changes must begin at the very highest levels. The Under Secretary of Public Diplomacy must have direct access to the President, be present during the development of foreign policy, and have a seat at National Security Council meetings.[70] This crucial input will provide insight into international reactions to proposed foreign policy initiatives and will help shape necessary preemptive public diplomacy strategies to gain greater reception to American influence abroad. Now is an ideal time for President Obama to establish this cultural change, thereby creating the standard for future administrations regarding the importance and relevance of U.S. public diplomacy in advancing national interests.[71] Such recognition by the Executive office will better delineate lines of authority, engender greater priority, and foster interagency cooperation for Public diplomacy initiatives.[72] As former prominent USIA director Edward R. Morrow warned, "Public diplomacy needs to be in at the take off of foreign policies, not just at the occasional crash landing."[73]

First, and foremost, the Under Secretary of Public Diplomacy and Public Affairs must coordinate all U.S. public diplomacy efforts. Unity of effort and interagency coordination of public diplomacy related programs within the White House, the DOD and the DoS, prevents irregular emphasis and competing priorities. Cooperation among departments facilitates successful implementation of U.S. foreign policy agendas. Synchronized strategy enables a streamlined, uniform

approach reducing the likelihood of both gaps and redundancy in various areas of effort or geographic regions.

Similarly, the Under Secretary of Public Diplomacy and Public Affairs must be in the direct chain of command for all public diplomacy efforts down to the very level of field officers. As discussed, a synchronized approach at all levels with clear mission objectives is essential to the success of any agenda. It is the responsibility of the Under Secretary to create, implement and then adjust strategy as necessary. Without the authority over all areas and assets of public diplomacy, the flexibility of implementing urgent changes in strategy is lost. Additionally, the potential for essential regions to go understaffed and field agents to lack a unified mission focus becomes a dangerous reality.

The training and recruiting public diplomacy field officers must receive greater emphasis within the DoS. Public diplomacy strategy is only as effective as its messengers. Having as few as 60% of field officers meet the most minimum standards in language proficiency of their host nation is a poor testimony to the effectiveness of any program. If field officers are not able to converse and interact fluently and seamlessly with their target population then credibility is lost, and so is the message they are trying to deliver. Given the intensity of the rancor that exists in Muslim regions, the United States can ill afford field officer vacancies due to understaffing. Similarly, if public diplomacy is the weapon of choice in the war of ideas recruitment of public diplomacy officers must receive far greater emphasis and priority.

Preparing a successful vision for U.S. public diplomacy in the war of ideas requires a return to Cold War era prominence in the national security strategy. A 2008 survey of USIA alumni argue precedent exists to warrant such action.[74] Seventy-two percent of those surveyed reported that public diplomacy was instrumental to the defeat of communism.[75] A similarly large majority (77%) echo that public diplomacy plays an equally critical role in today's conflicts.[76] These experts note the top six U.S. Public diplomacy priorities during the Cold War are the same public diplomacy priorities identified in today's war of ideas.[77]

At the height of the Cold War, the United States devoted nearly 10,000 employees and a $1 billion dollar budget to its public diplomacy

programs.[78] Additionally, public diplomacy served as an independent foreign affairs entity within the executive branch and boasted the most extensive global presence of any U.S. government agency.[79] Today's public diplomacy budget of $859 million and 1,332 public diplomacy officers are a meager shadow by Cold War standards.[80]

To make U.S. public diplomacy more effective in the war of ideas, the United States must regain its base of credibility; beginning with its allies. Recent international polling data indicates that, since the start of the GWOT, the United States has lost a substantial degree of influence globally, even among its closest allies.[81] In 2008 polls of America's traditional allies, Britain, France and Germany, only Britain showed a slim majority (53%) reporting favorable views of the United Stattes, with France (42%) and Germany (31%) reporting smaller minorities.[82] This data reflects a significant decline in United States favorability among these close allies, who in 2000 had each demonstrated large majorities reporting favorable views of the United States.[83]

Notably, the United States currently suffers unprecedented anti-Americanism in Western Europe, even in the United Kingdom where 41% of individuals polled believe that America is a greater threat to world peace than Iran.[84] Similarly, other allies such as Japan and Australia, where clear majorities held favorable views of the U.S. in 2000, reported steady declines in U.S. favorability since the beginning of GWOT to present.[85] In Turkey, a NATO ally, U.S. favorability ratings have plummeted from 52% in 2000 to 12% in 2008.[86] Similarly, only 13% of those polled in Turkey held favorable views of Americans.[87]

Equally concerning, of the 24 countries polled in the 2008 Pew Global Attitudes Project (GAP), 21 view the United States as having a predominantly negative influence in their country.[88] Nineteen of the twenty-four counties polled similarly reported the U.S. economy had a negative influence on their country.[89] Fortunately, most countries polled in the Pew GAP viewed Americans more favorably than the United States itself, indicating less hostility toward the American people.[90] A notable exception to this finding, however, occurred in the Latin American countries polled, Mexico, Argentina and Brazil, where strong negative views of the United States correspond closely with similar negativity directed against Amercian citizens.[91]

United States public diplomacy must also regain credibility with Muslim nations to succeed in the war of ideas. This strategy requires the United States to demonstrate its willingness to depart from past policies, transition away from the confrontational term, "war of ideas" and emphasize cultural connections with Muslim nations. Expanding U.S. public diplomacy programs to bridge relations with Iran is a bold strike, one likely to find success rebuilding U.S. credibility among Muslims.

United States engagment of Iran via public diplomacy is a formidable task; particularly when considering the significant number of Iranians who hold negative views of the U.S. government, but developing such relations is a cornerstone to progress in the war of ideas. Recent World Public Opinion.org polls demonstrate the critical nature of this goal. Specifically, 74% of Iranians feel the U.S. Government has a negative influence on the rest of the world.[92] While a large majority of Iranians (>80%) believe the United States seeks to control Middle East oil reserves for its own interests.[93] Eighty-four percent of Iranians believe the United States objectively seeks to weaken and divide the Islamic world.[94] Equally concerning, 64% of Iranians polled feel the United States intentionally desires to humiliate the Islamic world.[95]

Despite remnants of distrust between the two nations, Steven Kull, director of World Public Opinion.org, believes Iran is currently expressing a greater readiness to normalize relations with the United States, particularly in such areas as tourism, trade, and journalistic, educational, cultural and athletic exchanges.[96] His opinion stems from a significant decrease in hostility toward the United States illustrated by comparing polling data from 2006 and 2008 where the belief that violent conflict between the West and Muslims is inevitable, has dropped to 12% in 2008 compared to 25% in 2006.[97] Additionally, decreasing numbers of Iranians state the United States is a direct threat to their country and hostile to Islam (65% in 2006, vs. 51% in 2008).[98] Similarly, fewer Iranians consider U.S. military presence in the Middle East a direct threat against Iran (55% in 2008, down from 73% in 2006) or view Americans unfavorably (37% in 2008, down from 49% in 2006).[99] Equally reassuring, 76% of Iranians polled felt attacks against U.S. citizens in the United States was never justifiable.[100]

Perhaps more compelling is data suggesting that efforts to normalize relations with Iran may aid U.S. foreign policy objectives in the Middle East and mitigate concerns regarding Iranian nuclear weapons development. A majority of Iranians reported regional concessions and concessions with their nuclear energy program would be acceptable in exchange for normalized relations with the United States.[101] In fact, a majority of Iranians oppose nuclear weapons development with a near equal majority stating such weapons violate the principles of Islam.[102] Similar majorities endorse the Nuclear Non-Proliferation Treaty allowing the International Atomic Energy Agency full and permanent access to Iranian nuclear facilities in exchange for allowing Iran to conduct full-cycle nuclear energy production.[103] A majority of Iranians polled stated they would end support for armed anti-government groups in Iraq for normalized relations with the United States.[104] Twenty-four percent of Iranians expressed willingness to recognize the State of Israel.[105] That number nearly doubled when posed as a condition for normalizing relations with the United States.[106] Finally, the majority of Iranians had no desire for Iranian dominance within their region, preferring instead, the development of cooperative relations with surrounding Middle Eastern countries.[107]

Polling data collected in the United States and Iran also suggests majorities in both nations believe common ground, with similar wants and needs, exists between them.[108] Both Americans and Iranians view terrorism as a national threat and both have strong negative opinions toward Osama bin Laden.[109] Both the majorities of Americans and Iranians reject the concept of attacks against civilians.[110] A large majority of Iranians support the principles of free elections and freedom of the press.[111] Nearly equal majorities from each country (69% of Iranians and 73% of Americans) support bilateral discussions on ways to stabilize Iraq.[112]

The recent ease on U.S. restrictions regarding stem cell research by the Obama administration represents a poignant opportunity for U.S. Public diplomacy to initiate relations with Iran. Iran is an international leader in stem cell research whose scientists developed human embryonic stem cell lines as far back as 2003 and who, in 2008, devoted 2.5 billion in funding to the country's stem cell research over

the next five years.[113] In fact, several other Muslim countries, such as Malaysia, Egypt and Turkey, are also actively involved in their own stem cell research programs.[114] United States public diplomacy could conduct and orchestrate international scientific symposia devoted to the advancement of stem cell research and the development of global international ethics standards for such research.

Prior to any U.S. public diplomacy exchange with Iran, the United States must respect that polling data demonstrates a majority of Iranians are satisfied with their form of government.[115] Similarly, the majority of Iranians disapprove of U.S. attempts to spread democracy within Iran.[116] These data warrant further review by the DoS, who continues to identify promoting democracy as one of the primary objectives of U.S. public diplomacy.[117]

Success in the war of ideas may also require modifications to current foreign policy objectives. International opinion surveys demonstrate that much of the decline in America's image over the last several years surrounds opposition to recent U.S. foreign policy initiatives and its expanding global military presence.[118] Indeed, polling data of Muslim publics in the Middle East indicate wide support for the withdrawal of U.S. Forces from the Middle East, including U.S. naval forces in the Persian Gulf.[119] Similarly, international concerns exist that feel the build up of U.S. military presence in the Middle East over the last several decades actually exacerbates threats of nuclear proliferation and terrorism.[120] Ironically, while large majorities of Muslims polled disapprove of terrorist attacks against Americans, equal majorities support al Qaeda's methods of pressuring the United States to remove all its forces and bases from Muslim lands.[121] Large majorities view the U.S. military presence in the Middle East as a means to weaken and divide the Islamic world.[122]

Polls carried out in Iraq in 2008 also demonstrate a growing desire for decreased U.S. military presence in the region. Data indicates that the majority of Iraqis are impatient with the pace of U.S. military withdrawal.[123] Eighty-four percent of Iraqis polled desire the withdrawal of U.S. forces within a year.[124] Of particular concern, 71% of Iraqis feel the U.S. desires to occupy Iraq with permanent bases and 61% view the presence of U.S. forces in Iraq as destabilizing their

security situation.[125] Such findings are an ominous predictor of the Iraqi's willingness to cooperate with the coalition forces, or support an insurgency.[126] Sixty-one percent of Iraqis support attacks on U.S. troops, while 68% of Iraqis endorse non-military assistance by the United States, to include, building schools, health clinics and other assistance with organizing communities.[127]

While global opinion polls should not dictate any country's foreign policy, countries should not routinely dismiss them. As such, the U.S. should re-evaluate its military force structure in the Middle East. Phased reductions of American forces and bases in the Middle East based on a timetable ratified through the UN Security Council, demonstrates U.S. commitment to international governing bodies and multilateralism.

Conclusion

Concluding budget cuts and staff reductions alone account for U.S. public diplomacy's ineffectiveness in the war of ideas to date oversimplifies the greater complexity of issues at hand. Upon merging within the DoS, U.S. public diplomacy abandoned the very principles that define its functionality, independence, agility, coordinated action, a direct voice with the executive office, and person-to-person contact with target populations. Rather than appropriately vetting aggressive new foreign policy initiatives through U.S. public diplomacy, America blindly attempted to superimpose Western values upon an established foreign culture with predictable results to only then question, "Why do they hate us?" Lastly, America's apprehensions toward confronting ideological struggles led to a disproportionate emphasis for public diplomacy on pubic relations as opposed to confronting the more challenging issue of containing the spread of Islamic extremism.

Success in the war of ideas requires a comprehensive, coordinated, overarching strategy for U.S. public diplomacy, something lacking since the Cold War era. Rather than viewed as a relic of a past conflict, the success of public diplomacy (or USIA) during the Cold War era should serve as a template for the level of national commitment and emphasis necessary for public diplomacy to favorably influence the war of ideas.[128] International anti-Americanism and the spread of Islamic

extremism threaten U.S. interests globally and create a growing national security threat. The United States must prioritize its public diplomacy efforts to counter these threats. In order to do so it must engage in the war of ideas with as much vigor and capital as it dedicated to winning the Cold War.[129] Similarly, public diplomacy must regain the prominence it held during the Cold War era as a central component of national strategy and America's premiere political weapon to contain Soviet influence beyond its borders.[130]

As recent opinion polls indicate, Islamic extremism is losing favor in even the most conservative of Muslim countries. Now is the ideal time for the new administration to capitalize upon this momentum and redefine America's approach to the war of ideas. Rebuilding public diplomacy will enable the United States to distance itself from the ambiguous and arguably confrontational term, "war of ideas," and launch a new, inclusive direction aimed at creating cultural harmony with moderate Muslims.

National Communications Strategy

Colonel Suhail M. Alserraidi
United Arab Emirates

The time has come to look anew at our institutions of public diplomacy. We must do much more to confront hateful propaganda, dispel dangerous myths and get out the truth. We must increase our exchanges with the rest of the world. We must work closer than ever with educational institutions, the private sector and nongovernmental organizations and we must encourage our citizens to engage the world to learn foreign languages, to understand different cultures and to welcome others into their homes.

—Secretary of State Condoleezza Rice[1]

Nature of the Information Environment

The United States is and has been for the past eight years, engaged in a difficult long-term struggle against secular and religious extremists. This major struggle, especially in the Middle East, has shown that communication is a critical factor in overcoming extremists. The need to engage, enforce, inform, understand and influence people, not only overseas audiences but also the American public, has become vital.

However, at the beginning of this struggle the public diplomacy effort, especially for the Arab and Muslim world, reflected a system that was outmoded, lacked resources and had no strategic direction. The United States had previous successes in public diplomacy, such as the Fulbright education two-way exchanges, the Marshall Plan, the United States moon landing, and the reunification of Germany. In recent times, only the Reagan years had communication strategies that took a front role in all political challenges. The strategy was simple and clear with a mission "to win the Cold War once and for all" stated personally by President Reagan. Many people today expect public diplomacy to instantly produce goodwill among other nations without first establishing an atmosphere of trust and understanding. What is needed in this struggle with militants is presidential leadership, resources, and full commitment by the government and private organizations. To demonstrate the need for an effective strategic communication

strategy, the Heritage Foundation conducted a poll and stated in an article that "many in the Arab world believe that the United States wants to destroy Islam and replace it with Christianity."[2]

Strategic Intent

The strategic intent of strategic communication is to assist in winning the War on Terror by winning the battle of ideas. The battle of ideas is part of the overall public diplomacy strategy except its task is not to change foreign views of the United States and its policies, but to ensure that unfavorable sentiments and "day-to-day grievances toward the United States and its allies do not manifest themselves in the form of violent extremists."[3] The question of the primary mission for the battle of ideas is whether to defeat the terrorists or to build a long-term relationship of trust, understanding, and support for United States foreign policy objectives. Arab and Muslim nations may see the first choice as being taken advantage of for United States purposes. The second choice considers the Arab and Muslim world as long-term partners. To achieve the strategic intent of winning the war on terror we must choose to become full partners with Muslim nations. To accomplish this we must understand that overall United States policy is the most important part of the task. The United States cannot expect other nations to accept their policies if other nations don't understand them, have little or no input and disagree with the policies. Therefore, we must accept the fact that we need the assistance of other nations and people and their views, beliefs and interests. This begins with listening.

Goals and Objectives

The goal of strategic communication is to help defeat terrorism by producing counterterrorism ideas through words, deeds and images that separate terrorists from their base and general audiences. This will result in the avoidance of violence to achieve political objectives, ending attempts of radicalizing and recruiting new members and making those who do use violence isolated and condemned.

The objective of strategic communication is to be proactive, sustained with a coordinated and coherent set of actions that support United States strategic objectives. Some actions to achieve these objectives are:

1. Understanding of global attitudes and cultures. In reference to the Arab and Muslim world, the United States must understand that their societies and countries are diverse culturally, linguistically, ethically and religiously and thus the United States must customize their message and ideas to each nation.

2. Learn to listen. The United States needs to hear the voices of other nations, especially Arab and Muslim political sectors, not just pro-American groups. The United States needs to listen, address and interact with the Arab world and its different voices and be willing to have frank, truthful, respectful and tough discussions in which they, at times, must be ready to lose.

3. Understand the transformation of the media, especially with young adults. Information flow is primarily by viral methods such as Goggle, YouTube, Wikipedia, blogs, chat rooms, etc., and not broadcasts. The focus is not on the delivery means but on what the content of the message is and its credibility to the people. Terrorist organizations have used the media to their advantage through fast responses, flexibility, decentralized leadership and local autonomy. They recognize that bad news is "good" since bombs sell and schools don't. The rise of pan-Arab media outlets have vastly increased (e.g., Al-Jazeera) and the web is available to all. The traditional media are losing their influence to the citizen reports on new media. Censorship or hiding of information has become impossible, and balanced, validated reporting has changed to polarized, target group reporting.

4. The world today is watching the deeds and actions of the United States to compare them with United States strategic communication messages. Communication today is global and "bad" actions are quickly seen and measured. Also, domestic messages sent for support at home can have a negative result internationally. The United States must also understand that what they say at times is not what others hear. Concepts such as "democracy," "rule-of-law" and "freedom" have different meanings in different cultures. The United States value system is confusing to others, especially in the Arab and Muslim world, particularly considering United States cultural homogeneity vs. cultural diversity and the acceptance of

alternate lifestyles. Thus, the focus of the United States message should be cultural concepts that are globally valued such as human dignity, health, personal safety, environment, education and economic well-being.

Conclusion

The battle of ideas will be a continuing challenge to the United States. The nation must mobilize and utilize its best talent, expertise and resources both within and outside the government. It needs a national structure for strategic communication, increased financial support and strong leadership from the highest levels. Fortunately, the new United States President may be up to all the challenges. His decision to make his first official interview as President on the Arabic television station, Al-Arabiya, shows his understanding of culture, respect and value of dialogue. President Obama's comments at the G-20 Conference of "listening to others" brings the promise of a fresh start in U.S.-world relations. His Secretary of State, Hillary Clinton, comments on "smart power"[4] which she defines as relying heavily on global engagement and public diplomacy also shows that the United States will not act unilaterally as it has in the past.

The understanding, support and leadership for United States strategic communication is rising. This is proven by the introduction in Congress of the "Strategic Communication Act of 2009" by Republican William Thornberry (R-TX-13) on January 31, 2009. The subtitle states "to improve the conduct of strategic communication by the Federal Government."[5] Once again, the United States is rising to a challenge.

Section Two

Information Effects through Network and Knowledge-based Operations


Prudens
Futuri

Introduction

William O. Waddell
Director, Command and Control Group
Director, Cyberspace Operations Group
Center for Strategic Leadership
U.S. Army War College

Section two is focused on the practical application of existing information theories and concepts concerning information availability and its usage in national and theater operations. Since the onset of the information age, activities and considerations involved in the protection, availability and application of information have been debated and put into theory; however these theories become somewhat archaic after time since the information environment continues to present an ever changing medium. Starting with the concept of Net-Centric Warfare developed in 1998 and the Joint Vision series (2010 and 2020) many new information related conceptual ideas have emerged and taken root in military planning and operations. While the initial concepts still have some merit, they need to be "rounded out," updated, and refocused. Protecting information that rides the information super-highway has moved up to front and center in national and strategic considerations, as vulnerabilities in military networks and the commercial internet raise significant threats to the well being of the U.S. culture. Additionally, empowering military and government agencies with the timely flow of accurate information, and developing "knowledge" from that information is a full time issue as empowerment involves more than just getting the information to the right location. Finally, the development of repositories of critical and historic information that is available to a ubiquitous audience, while maintaining the appropriate level of security will move military planners and decision makers to new levels of success. Each of these authors explores one of these concepts as they present their thesis on how to improve information protection, flow, and availability.

The first monograph, written by Lieutenant Colonel Scott W. Beidleman explores the protection aspect of information requirements,

writing about the potential for cyber attack to cause exceptionally grave damage to a state's national security, and examining what issues would make a cyber attack an act of war. He considers efforts to apply existing international norms to cyberspace, and also assesses how traditional concepts of deterrence apply in cyberspace. He concludes that cyber attack, under certain conditions, must be treated as an act of war; that deterrence works to dissuade cyber aggression; and provides recommendations to protect American national interests.

Next, Colonel David A. Barlow argues that the requirement for unimpeded information sharing is a central tenet of network centric warfare and is not currently a reality across theaters of operation. He further contends that the different combatant command information technology support methodologies impede network centric operations within the Department of Defense. His paper examines desktop collateral information technology support to the combatant commands as it pertains to network centric warfare at the theater level, and proposes a single solution provided by a single agency to service all ten combatant commands. By examining the strengths and weaknesses of the current support methods he provides strategic recommendations aimed at improving network centric warfare.

Lieutenant Colonel Robert B. Sofge writes that Knowledge Centric Warfare, an evolutionary step beyond Network Centric Warfare, provides a conceptual underpinning to propel a fundamental shift in the joint force as it focuses on knowledge vice information. Built upon the philosophical position that knowledge is inseparable from the knower, this paper rejects the objectification of knowledge and argues that deliberately developing the private and cultural mental models of the force will achieve the Chairman's vision.

Finally, Commander Timothy L. Daniels writes that knowledge created and shared within and among responsible organizations enables timely and effective problem solving, decision-making, and action critical to successful Security, Stability, Transition, and Reconstruction Operations (SSTRO) in complex and uncertain environments. He explores knowledge management as an SSTRO enabler and examines the use of the Intelligent Complex Adaptive System (ICAS) Model to demonstrate strategic Knowledge Management (KM) application. Additionally, he

explores organizational culture as a barrier to KM implementation and identifies strategic leader focus areas for overcoming cultural barriers. Finally, he provides recommendations for realizing the strategic utility of KM as part of SSTRO to achieve national security objectives.

These excellent papers provide a depth of research and thought concerning the future development of information processes and network structure. They lay the groundwork for the development of new and innovative ideas to meet the information requirements emerging in future military and commercial ventures.


Prudens
Futuri

Defining and Deterring Cyber War

Lieutenant Colonel Scott W. Beidleman
United States Air Force

Cyberspace is the nervous system—the control system of our country.
—President George W. Bush[1]

What if one day the control systems of a major dam suddenly released torrents of water upon nearby communities, or safety systems of nuclear power plants malfunctioned, or air traffic control systems of major airports shut down, or financial transactions of major banks and stock exchanges stopped or disappeared? What if these events happened simultaneously? Is such a scenario the plot of a Hollywood blockbuster, or the new reality of twenty-first century cyber war?

Since the public debut of the Internet in the early 1990s, not all users have acted with peaceful purposes in cyberspace. The magnitude and frequency of cyber attacks have grown continuously since the inception of the World Wide Web, from the nuisance of individual hackers in the early years to potential state-sponsored cyber aggression recently against Estonia and Georgia. Indeed, cyberspace has emerged as a setting for war on par with land, sea, air, and space. This is unsettling since the Internet and information and communications technologies (ICT) have increasingly become integrated into all aspects of human society. In fact, computers control much of America's critical infrastructure and essential processes in manufacturing, utilities, banking, and communications.[2] Even President Bush declared cyberspace as America's nervous system and the control system of the country.[3] Cyberspace is America's operating system, analogous to a national-level Windows XP. A system crash would cause grave damage to the economy and national security, and rebooting America might not be easy. Consequently, this paper asserts that cyber attacks have the potential to cause grave damage to the national security of the United States and must be treated as an act of war. As a first line of deterrence in this relatively new domain of

war, the United States should lead efforts to establish an international regime of laws, norms, and definitions to deter aggression in cyberspace.

The question of cyber deterrence reveals several more fundamental questions, the answers to which the international community has not reached consensus. Does cyber attack constitute a use of force? Is cyber attack an act of war? Do the traditional concepts of deterrence prevail in cyberspace? These questions are difficult to answer because there are no common, codified, legal standards regarding cyber aggression. More than a decade after the advent of the Internet, the international community still has no sanctioned body of norms to constrain states' actions in cyberspace.

This paper begins by examining the increasing scope and destructiveness of cyber attacks and establishing cyber war as a threat to the national interests of the United States. Next, it defines cyber war and attempts to assess cyber attack as an act of war regarding current international law. Then the study applies the traditional concepts of deterrence to cyberspace and concludes with recommendations. The research concludes that deterrence can work in cyberspace, but the United States must pursue a comprehensive approach that combines the fielding of defensive and offensive cyber capabilities with a concerted effort to establish an international regime to constrain cyber aggression.

A Threat to National Security

Since its arrival as a public domain in the 1990s, the Internet and ICT have become integrated into all aspects of human society. Advances in ICT continuously fuel globalization, which increases the interdependence of states' economies, politics, and security. Concurrently, it increases states' vulnerabilities to cyber attack. Like any other medium, cyberspace provides avenues to pursue peaceful ends as well as aggression.

One of the earliest attacks in cyberspace to gain notoriety occurred in 1994 at Rome Lab, a military research and development laboratory. Two hackers intruded into the lab's network 150 times but caused no damage.[4] One of the hackers from Israel was acquitted because no Israeli laws applied to the incident.[5] A few years later the Love

Bug virus infected over 60 million computers worldwide and caused organizations as diverse as the British Parliament and the Ford Motor Company to shut down their servers.[6] Again, the Filipino perpetrator was not charged or punished because "creating computer viruses was not a crime under Philippine law."[7]

In 1997, the U.S. military conducted Eligible Receiver, the nation's first information warfare exercise. This exercise tasked a group of highly trained computer experts, known as a government red team, to independently examine plans and operations from the perspective of adversaries.[8] The red team "was able to infiltrate and take control of Pacific command center computers, as well as power grids and 9/11 emergency systems in nine major U.S. cities."[9] These results suggested that America's critical military and civilian infrastructures were highly vulnerable. In fact, the very next year hackers confirmed the findings of Eligible Receiver when they attacked Department of Defense networks and compromised over 500 computers in an incident dubbed "Solar Sunrise."[10] This attack targeted logistics and accounting systems essential to managing and deploying U.S. military forces at a time when the United States was considering military action against Iraq for their failure to comply with United Nations' (UN) resolutions.[11] These events served as signs of things to come as smaller-scale hacker-level assaults gave way to more organized and destructive attacks, escalating to reputed state-level attacks on Estonia and Georgia.

Since Estonia declared independence from the Soviet Union in 1991, it has zealously embraced information and communications technology and has become one of the most wired nations in Europe. More than 65 percent of Estonians have access to the Internet and they conduct virtually all of the administrative functions of their society online.[12] This includes 97 percent of their banking transactions, as well as voting and paying taxes online.[13] In fact, Estonia has embraced cyberspace to such a high degree that all of its citizens carry national identification cards embedded with electronic identity chips and the country's parliament declared Internet access a basic human right in 2000.[14] This high degree of reliance on ICT made Estonia extremely vulnerable to cyber attack.

For two weeks beginning in late April 2007 this eastern European nation endured the world's first cyber attack that threatened the national security of an entire state.[15] The persistent attacks involved computer robot networks, known as botnets, that seized more than a million computers from 75 countries and directed them to barrage targets in Estonia, eventually "bringing the functioning of government, banks, media and other institutions to a virtual standstill."[16] The majority of the attacks came in the form of distributed denial of service (DDOS) attacks that overwhelmed websites with a massive number of requests for information and crippled the underlying network of routers and servers.[17] Although Estonian officials said the sources of the attacks had possible ties to the Russian government, insufficient evidence existed to accuse Moscow formally. While the investigation continues, so far only one person has been convicted and fined in the cyber attack against Estonia.[18]

A year after the Estonia attacks, Georgia suffered the world's first cyber attacks that coincided with conventional attacks.[19] The cyber attacks were staged to begin shortly before the initial Russian airstrikes as part of the Russian invasion in August 2008.[20] The attacks focused on government websites, with media, communications, banking, and transportation companies also targeted.[21] These botnet-driven DDOS attacks were accompanied by a cyber blockade that rerouted all internal Georgian Internet traffic through Russia and blocked electronic traffic in and out of Georgia.[22] The impact of the cyber attacks on Georgia was significant, but less severe than the Estonia attacks since Georgian society is a much less dependent on the Internet. These attacks severely limited not only Georgia's ability to communicate to the world and its own people, but also its ability to shape international perception while fighting a war in which "accusations of genocide have been levied."[23] Similar to the Estonian attacks, circumstances suggested Russian involvement, but there was no hard evidence to substantiate its complicity. However, experts believe the cyber attacks bore "the markings of a trained and centrally coordinated cadre of professionals," and "were too successful to have materialized independent of one another."[24] As evidenced by the cyber attacks on the two former Soviet republics, greater dependence on cyberspace equates to greater vulnerability.

In the United States, where Internet use has penetrated 73 percent of the American population, cyberspace plays a vital role in controlling critical infrastructure and processes in manufacturing, utilities, banking, and communications, as well as military systems.[25] Recognizing this vulnerability, President Bush declared that a healthy, functioning cyberspace was essential to U.S. national interests.[26] In fact, cyber aggression threatens three of the four core U.S. national interests as defined by the U.S. Army War College: security of the homeland, economic well-being, and a stable international order.[27]

The critical infrastructure of homeland security is extremely reliant on ICT, specifically the supervisory control and data acquisition (SCADA) systems. SCADA systems are the computer systems that use ICT to monitor and adjust switching and other processes of critical infrastructures like power plants. These systems are frequently unmanned and are remotely accessed by engineers via telecommunications links.[28] The Chairman of the Joint Chiefs of Staff recognized the destructive potential of cyber attacks against critical infrastructures and compared cyber war with weapons of mass destruction when he stated,

Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction (WMD) or methods producing WMD-like effects. Such catastrophic effects are possible in cyberspace because of the existing linkage of cyberspace to critical infrastructure SCADA systems. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructures locally, nationally, or possibly globally.[29]

The corresponding vulnerabilities have not gone unnoticed. Al Qaeda computers seized in Afghanistan contained models of a dam complete with engineering software that "enabled the simulation of a catastrophic failure of dam controls," as well as "programming instructions for digital switches that run power, water, transport, and communications grids."[30] Additionally, in late 2001 the FBI uncovered multiple cases of electronic surveillance of "emergency telephone systems, electrical generation and transmission equipment, water storage and distribution systems, nuclear power plants, and gas facilities across the U.S." emanating from Saudi Arabia, Indonesia, and Pakistan.[31] Furthermore,

hackers frequently employ malicious computer code known as worms, to identify and exploit vulnerabilities within a network.[32] In one such instance, the "Slammer" computer worm corrupted the safety monitoring systems of a nuclear power plant in Ohio for five hours in 2003 by exploiting a program code backdoor through the Internet.[33] Another worm known as MSBlast was reportedly linked to the major power outage that hit the northeast United States in August 2003, where it "crippled key detection systems and delayed response during a critical time."[34] In 2007, researchers at the Idaho National Laboratory "launched an experimental cyber attack" causing a generator to self-destruct by changing the device's operating cycle.[35] Industry experts hypothesize that "cyber attacks on key electrical facilities could knock out power to large geographic areas for months, harming the nation's economy."[36]

Like homeland security, economic well being is another national interest that has serious vulnerability to cyber attack. The global economy is linked to U.S. and international financial systems controlled by computer networks. In fact, "finance, wholesale and retail trade, transportation, much of manufacturing, and many service industries would slow to a crawl without computers."[37] Estimated economic losses due to cyber attacks amounted to $226 billion worldwide in 2003.[38] The average corporation traded on the New York Stock Exchange suffered losses up to five percent in the days following an attack, which translated into shareholder losses up to $200 million.[39] In 2006, a jihadist web site promoted an aspirational threat to "carry out cyber attacks on the U.S. financial industry to retaliate for abuses at the Guantanamo Bay prison facility."[40] One year later, the aforementioned cyber attack on Estonia forced two major banks to suspend operations, resulting in the loss of millions of dollars.[41] Similarly, the attacks on Georgia's banking system in August, 2008, shut down electronic financial transactions for 10 days.[42] Certainly, global financial markets are volatile enough without the added disruption and uncertainty of cyber attacks. A successful major attack on a primary financial center like Wall Street or the Nikkei would not only damage economies worldwide, but also likely induce fiscal panic for anyone concerned about their pensions and life savings, as well as severely damage peoples' faith in their governments.

In addition to damaging security and economic well being, cyber aggression can adversely affect a stable international order, as the cumulative damage from cyber attacks against critical infrastructure "…can ignite panic, cause a loss of confidence, create uncertainty, and destroy trust in modern society."[43] Sustained disruptions to basic services could lead to a mob mentality. "The fragility of social order was demonstrated in 2008 when fuel price increases led to widespread violent protests across the globe."[44]

In short, since the inception of the Internet, cyber attacks have grown in scope and destructiveness to where they may now threaten America's core national interests of homeland security, the economy, and international stability. In fact, aggression in cyberspace has emerged as a threat to the national security of all sovereign states. However, "there is currently no international, legally binding instrument that would address cyber attacks as threats to national security."[45] Given this, can cyber attack threaten national security and not be considered an act of war?

Cyber Attack as an Act of War

States exist in an anarchic world where security is a self-help system. States maintain order and security by exercising their monopoly on legitimate violence.[46] This legitimacy is derived and defined by the international regime of laws, norms, and definitions regarding war and aggression. Therefore, international stability is underpinned by a common understanding of this regime that ultimately frames how states behave in the anarchic system. Similarly, definitions of cyber war and related terms are critical to how the laws of war and international treaties proscribe the scope and use of cyber capabilities for martial purposes.[47] In other words, norms and definitions guide how states should behave in cyberspace. Uncertainty caused by the lack of a common understanding regarding cyber attack could escalate conflicts unintentionally if states have different interpretations of what is permissible in cyberspace.[48] A common understanding of cyber war can also guide how a state deters cyber attacks. For clarity and consistency, a definition of cyber war must be preceded by a definition of cyberspace.

Defining cyberspace is a challenge due to its expansive and global nature and the rapid rate of change of ICT. Dr. Dan Kuehl, an information operations expert at the National Defense University identified over a dozen definitions of cyberspace in circulation, ranging from Google's "the place between the phones" to several variations within the Department of Defense.[49]

The Department of Defense definition has matured over time. Early joint doctrine limited cyberspace to "a notional environment in which digitized information is communicated over computer networks," implying cyberspace was simply a communications medium of a theoretical or imaginary nature.[50] In 2006, the Chairman of the Joint Chiefs of Staff referred to cyberspace as a "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures," which recognized cyberspace as a domain that stretched beyond computers.[51] In the same year, the Air Force's Cyber Task Force more bluntly deemed cyberspace as an operational warfighting domain where the electromagnetic spectrum was the maneuver space.[52] Finally, the October 2008 update of Joint Publication (JP) 1-02, the official military dictionary, refined cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[53] This definition in JP 1-02 provides a solid basis for defining cyber war. In addition to recognizing the omnipresent nature of cyberspace, this definition references the information environment, inferring cyberspace pervades and links the physical world, where people and society's critical infrastructures reside, the information realm, where data is created and stored, and the cognitive realm where human perceptions and decisions are made.[54] These linkages make cyber warfare an attractive supplement or alternative to conventional war and tie cyberspace to national security.

President Bush underscored the national security implications of cyberspace when he characterized it as the nervous system of the nation's critical infrastructures, controlling public and private institutional assets in the "agriculture, food, water, public health,

emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping" sectors.[55] The president specifically stated cyberspace "is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work."[56]

From this definition and its implications, one could deduce that cyber war is simply warfare in the cyberspace domain, but this simplification is insufficient for two reasons. First, 'warfare in cyberspace' is too broad a definition. Dropping a bomb on a telecommunications center is not cyber war. Moreover, cyber war is not synonymous with information operations (IO), but it could be a subset since IO is comprised of psychological operations, military deception, operations security, electronic warfare, and computer network operations (CNO).[57] CNO involves actions through "the use of computer networks" to attack "information resident in computers and computer networks, or the computers and networks themselves."[58] Cyber war uses cyberspace to attack personnel, facilities, or equipment in addition to information and computers.[59]

Second, defining cyber war as warfare in cyberspace ignores the complexity of applying the more fundamental legal aspects of war to cyberspace. What is war in cyberspace? The original drafters of international law did not envision situations created by cyber capabilities and the current regime of international law is still not comprehensive in this regard. Currently, the UN Charter, Hague and Geneva Conventions, and related treaties are the only basis from which to assess acts of war.

International law does not define the term "act of war." In the sense that war is "the legal consequence of the use of force" between states, international law is organized on the concepts of "use of force" and aggression.[60] A state of war may exist when a nation violates Article 2(4) of the UN Charter. Article 2(4) prohibits states from threatening or using force "…against the territorial integrity or political independence of any state."[61] However, not all force is prohibited. The Charter outlaws the use of aggressive force while recognizing the right of states to use force in self-defense as specified in Article 51.[62] The term aggressive

generally refers to the actions of the first party resorting to force or the threat thereof.[63] Furthermore, the UN defines aggression in Article 1 of the UN General Assembly Resolution 3314 as "the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another state."[64] Thus the "trigger for the inherent right of self-defense" that defines a legal state of war "is contingent on a use of force amounting to an armed attack."[65] So the key issue in understanding cyber war involves the concept of armed attack.

Unfortunately, the UN Charter does not provide a definition of armed attack to apply to cyberspace. However, the General Assembly's Resolution 3314 provides several examples of aggression that constitute armed attack.[66] Such actions include invasion or attack, bombardment, blockade of ports or coasts, and attacks on land, sea, or air forces of another state.[67] These examples manifest themselves in the physical world and fall within the traditional approach of kinetic means of attack that produce physical effects on a state and its sovereignty. How does one translate these ideas into cyberspace where the concept of kinetic means does not easily apply?

In cyberspace, cyber attack is the mechanism that equates to the use of force. Cyber attack, although not defined officially, can be viewed as a subset of cyber operations employing the hostile use of computers and information technology infrastructure to achieve effects or objectives in or through cyberspace.[68] Cyber war occurs when cyber attacks reach the threshold of hostilities commonly recognized as war by the international community and defined by international law. While cyber attacks are hostile acts in cyberspace, not all cyber attacks equate to armed attack. Cyber attacks can range from the defacing of individual web sites to the organized shut down of electrical power grids, but defacing web sites hardly amounts to an act of war. Cyber attacks can target individuals, objects, or entire societies, and their effects can range from mere annoyance to physical destruction and death.[69] Somewhere along this spectrum of conflict in cyberspace, a cyber attack crosses the threshold and becomes an armed attack.

A logical discriminator to gauge a cyber attack is to judge the action by the effect or consequence it produces, rather than its means of delivery. "Armed attack should not be defined by whether or not kinetic energy

is employed or released, but rather by the nature of the direct results caused."[70] This is supported by international law which recognizes that the use of "unarmed, non-military physical force" can produce the same severe effects as an armed attack, so actions like the "spreading of fire across a frontier" or the "diversion of a river by an upstream state" would constitute armed attacks in terms of Article 2(4) of the UN Charter.[71] Cyber attacks may not exactly fit the unarmed, non-military physical force paradigm, but they can cause commensurate effects.

Following this logic, any cyber attack that causes the same level of damage as a traditional armed or kinetic attack, either through the destruction of physical property or loss of life, would be considered an armed attack. Whether a power plant is bombed by aircraft or its electrical grid destroyed by malicious code, a blackout is a blackout. Until recently this quantitative approach towards assessing cyber attacks achieved consensus among legal scholars.[72] However, cyber attacks can cause damage to other aspects of society besides physical property and people. As seen in Estonia and Georgia, a cyber attack can inflict economic and psychological damage as well. Scholars argue that an effects-based approach to classifying armed attack is not congruent with the qualitative and instrument-based paradigm of the UN Charter that places greater restrictions on military activity versus non-military activity.[73] For instance, a long-term, devastating economic embargo that causes enormous suffering would not be considered an armed attack, but a minor, armed border incursion would equate to an armed attack.[74] One method that attempts to bridge this quantitative and qualitative gap and may provide a more comprehensive assessment of cyber attack is known as Schmitt Analysis.

In 1999, Professor Michael N. Schmitt created a framework that can be used to assess whether a cyber attack equates to a use force in terms the UN Charter. For a given attack scenario, the method evaluates seven qualitative factors and produces a cumulative score that "determines the overall level of forcefulness, which is either above or below the Article 2(4) threshold" of the UN Charter.[75] Some of the more pertinent factors include severity, which measures the level of physical injury or damage to property; immediacy, which evaluates how fast the effects are seen; directness, which measures to what extent the attack is the

sole cause of the effect; and invasiveness, which assesses to what degree the attack crosses into the targeted state.[76]

In 2003, a team of researchers applied the Schmitt Analysis to a notional cyber attack scenario where terrorists remotely used malicious code to strike the software-intensive control systems of the Washington D.C. subway.[77] The simulated attack caused several train collisions, killing 30 people and causing extensive property damage. The analysis concluded that an armed attack occurred. It is clear that any cyber attack that produces effects tantamount to traditional armed force will score above the threshold of an armed attack. What is not clear is the case of cyber attacks that cause extreme economic damage. The severity factor of the Schmitt Analysis is designed to weigh physical destruction heavier than economic impact. Also, since most cyber attacks would emanate from outside the targeted state, cyber attacks earn lower invasiveness scores than traditional armed attacks, as was the case in the subway scenario.[78] The economic impacts of the Estonian and Georgian cyber attacks were considerable and they illustrate the potential for more devastating future attacks on economies. As this potential develops, the Schmitt criteria applied to cyber attack may need to adjustment.

International law is also unclear regarding acts of economic coercion. The prevailing view among scholars interpreting Article 2(4) of the UN Charter is that the charter only prohibits armed force and would not proscribe acts of economic coercion.[79] Alternatively, some scholars suggest economic coercion becomes economic aggression if the action jeopardizes a state's security.[80] A cyber attack of this consequence would meet the Article 2(4) threshold for a use of force, but probably not the armed attack threshold for self defense in Article 51.

Given its potential to cause grave damage to national security, cyber attack must be treated as an act of war, or in terms of international law, as a "use of force" and an armed attack. However, assessing whether a cyber attack is actually an act of war is a complicated effort. Each case must be examined in its own context against international laws and circumstances because no single rule set exists that defines what constitutes a use of force or armed attack under all circumstances.[81] Furthermore, the current regime of international laws, norms, and definitions were designed a half century before the advent of cyber

capabilities and thus are not well suited for cyberspace application. Existing international law impedes the development of a common understanding of cyber aggression and hinders a state's ability to deter cyber attacks against them.

Deterring Cyber War

In general, deterrence is a state of mind. It is the concept of one state influencing another state to choose not to do something that would conflict with the interests of the influencing state. Similarly, the central idea of deterrence from the perspective of the Department of Defense is "to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against U.S. vital interests."[82] Deterred states decide not to take certain actions because they perceive or fear that such actions would produce intolerable consequences.[83] The idea of influencing states' decisions assumes that states are rational actors "willing to weigh the perceived costs of an action against the perceived benefits, and to choose a course of action" logically based on "some reasonable cost-benefit ratio."[84]

Thus the efficacy of cyber deterrence relies on the ability to impose or raise costs and to deny or lower benefits related to cyber attack in a state's decision-making calculus. Credible cyber deterrence is also dependent on a state's willingness to use these abilities and a potential aggressor's awareness that these abilities as well as the will to use them exist. While a state's ability to deter cyber attacks is a subset of its overarching defense strategy comprised of all instruments of national power, this paper focuses on states' actions to deter cyber attack within the cyberspace domain. Effective cyber deterrence in cyberspace will employ a comprehensive scheme of offensive and defensive cyber capabilities supported by a robust international legal framework.

Offensive capabilities are the primary tools used to impose or raise costs in deterrence. Offensive cyber capabilities and operations provide a state the means and ways for retaliation and enhance the perceived probability that aggressors will pay severely for their actions. A more robust capability translates to a more credible imposition of costs. Until recently, U.S. efforts to develop offensive cyber capabilities have lagged

efforts on the defensive side. The daily onslaught of attacks on U.S. networks, coupled with the likelihood that potential U.S. adversaries will be less dependent on electronic networks than the United States, has prioritized activities for gathering intelligence and defending U.S. capabilities over those for disrupting enemy capabilities.[85] However, the United States has recently gained momentum in the development of offensive cyber capabilities.

In 2006, the United States published the *National Military Strategy for Cyber Operations* with the expressed intent to achieve "military strategic superiority in cyberspace."[86] One of its main goals is to ensure "adversaries are deterred from establishing or employing offensive capabilities against U.S. interests in cyberspace."[87] Unlike the air, land, and sea domains, the United States currently lacks dominance in cyberspace.[88] In fact, without a significant effort, the United States will lose its current technological advantages and "risks parity with adversaries" in cyberspace.[89] To this end, the United States has taken measures in support of offensive cyber operations. While each military service has some form of cyber footprint, the U.S. Air Force has incorporated operating in cyberspace as part of its core mission on par with flying and space operations. For instance, the commander of the Air Force's provisional cyber operations command envisions initial offensive cyber operations as subduing or killing data packets that threaten U.S. systems, with the potential to expand in the future to missions normally executed by conventional forces in the past.[90] The United States continues to modernize its cyber forces, create new hacker units, and conduct cyberwar exercises,[91] with the intent to "penetrate and disrupt foreign computer systems."[92] However, the United States is not alone in pursuing cyber attack. Over 120 countries already have or are developing computer attack capabilities, reinforcing the need for a strong defense.[93]

In addition to offensive means, defensive capabilities play a critical role in deterring cyber attack. Defensive cyber capabilities not only ensure essential services and functions of society continue unabated, they also deny or lower the benefits an aggressor might obtain via cyber attack. Defensive cyber capabilities increase a state's resistance to attacks and reduce the consequences of attacks. They enable the

state to strengthen the security of potential targets and correspondingly limit or eliminate an aggressor's ability to threaten the state through cyberspace. Ultimately they reduce the probability of success that an aggressor will achieve its goals.

The United States has employed a defensive cyber policy as outlined in the *National Strategy to Secure Cyberspace*. This strategy focuses on preventing cyber attacks against America's critical infrastructures, reducing national vulnerability to cyber attacks, and minimizing damage and recovery time from attacks that do occur.[94] It recognizes the need to unite all levels and facets of government with private industry and individual Internet users to fully integrate defensive efforts. Also, it outlines broad, robust defensive measures and capabilities to deter cyber attack. For instance, the United States continues to invest in defense of cyberspace infrastructure by "diversifying and limiting the number of access points that could be used for an attack."[95] Also, the Department of Homeland Security (DHS) is leading integrated efforts between the public and private sectors, like the U.S. Computer Emergency Readiness Team designed to analyze threats and coordinate responses to cyber attacks.[96]

However, the current U.S. approach focuses on deterring attacks in American cyberspace, implying that cyberspace recognizes state borders. Cyber attacks against the infrastructure or economies of other states can have severe effects that cascade to the United States. The globalized interdependence of cyberspace underscores the adage 'a risk accepted by one is a risk assumed by all,' thus implying that cyber aggression requires a cosmopolitan solution. Unfortunately, U.S. deterrent strategies do little to foster the crafting of international standards for state behavior in cyberspace. In contrast, Estonia, a veteran of the largest cyber attack in history, promotes a defensive strategy to secure cyberspace with a broader perspective. Like the United States, Estonia seeks to protect its critical infrastructure, to prevent cyber attacks, and to ensure a swift recovery of systems should an attack occur.[97] However, Estonia also champions the development of international norms to regulate cyber attacks.[98]

Over and above offensive and defensive cyber capabilities, the most critical component of a comprehensive approach to deter cyber attack is a robust international legal framework that addresses cyber aggression.

International law and norms are fundamental to deterrence because states "share an interest in adopting or codifying common standards for the conduct of international transactions…or in promoting or banning specific kinds of behavior by" states.[99] Multilateral agreements provide the most efficient way of realizing these shared interests.[100] The common acceptance of norms moderates state interaction and makes state behavior more predictable, which leads states to "combine to insist on respect for specific norms of…conduct by those who violate their consensus."[101] In this way, international law builds the framework that guides how and when states employ offensive and defensive cyber capabilities and forms the foundation of cyber deterrence. International law adds certainty to punitive actions and amplifies the costs of cyber attack by engendering a negative response from the entire international community, not just from the attacked state. Moreover, it adds credibility to the threat of reprisal by providing legitimacy to retaliatory actions and by increasing the potential to isolate the aggressive state. Also, international law provides a measure of protection to states that lack robust defensive and offensive cyber capabilities and serves as their first and possibly only line of deterrence.

However, recall that there is currently "no binding international law on cyber security" that "expresses the common will of countries."[102] In fact, the lack of international norms, laws, and definitions to govern state actions in cyberspace has created a gray area that can be exploited by aggressive states as long as their actions skirt the imprecise thresholds contained in the UN charter.[103] For example, in response to accusations of state-sponsored cyber war against Estonia, "the head of the Russian Military Forecasting Centre stated that the attacks against Estonia had not violated any international agreements because no such agreements exist," suggesting that even if Russia's complicity could be proved, Estonia's options for reprisal were limited.[104] Such an environment thwarts deterrence because it lowers the probability "of reprisal even if the attacker's identity is suspected" and reduces an attacker's potential costs of pursuing cyber attack.[105] Oddly, this void in international law is unique to cyberspace.

Historically, each time warfare was introduced to a new domain, international law reacted by developing domain-specific guidance in

some form of treaty or convention. For example, the rules governing actions on the seas have existed as customary law for centuries, based on the Grotian doctrine of 'freedom of the seas' dating back to the early 1600s.[106] This customary law now exists as the United Nations Convention on the Law of the Sea. Also, five years after World War I, the war in which the airplane made its debut as a weapon, the international community drafted the 1923 Hague Rules of Aerial Warfare. Although not ratified, these rules have endured to "form the basis of all current regulation of air warfare."[107] Moreover, ten years after the launch of Sputnik, the international community agreed to the principles of the Outer Space Treaty in 1967. Despite these precedents, roughly 16 years after the World Wide Web burst onto the public scene, no international regime exists to govern state actions in cyberspace.[108]

In addition to a lack of regulatory framework, ineffective attribution of cyber attacks further undermines deterrence in cyberspace and widens the exploitable gray area. The threat of offensive cyber capabilities will not deter aggression if the attacked state cannot identify its attacker. Likewise, deterrence falters if the UN cannot identify where to target sanctions. In the aftermath of the Estonian attacks, "neither NATO nor European Commission experts were able to find any proof of official Russian government participation."[109] This would reduce the probability of legitimate reprisal to zero and nearly eliminate the costs of pursuing cyber attack. Reversing this recurring theme in cyber attack investigations requires significant international investment.

In summary, the concept of deterrence is applicable to cyberspace since it focuses on the decision calculus of a state, not the domain in which it is employed. While offensive and defensive cyber capabilities are critical to deterring aggression, employing these capabilities depends on robust international norms for state behavior in cyberspace. International law is the first line of deterrence in cyberspace.

Conclusions and Recommendations

Since the launch of the information superhighway in the 1990s, the destructiveness of cyber attack has grown consistently in magnitude to the extent that it can now threatens the critical infrastructure that

forms the basis of modern society. In short, cyber attack can cause grave damage to national security. In fact, it can prevent a state from functioning.[110] Rational thought realizes cyber attack can be an act of war, but common sense and the rule of law can conflict in cyberspace. The current regime of international laws, norms, and definitions is not only insufficient to address cyber aggression, it actually intensifies the dangers of cyber attack by creating a gray area of legitimacy that can be exploited by cyber aggressors. This loophole, coupled with insufficient techniques to identify assailants, undermines a state's ability to deter cyber attack. To reverse this trend, the United States must pursue a policy of changing the existing regime which in this case refers to the "complex of norms, treaties, international organizations, and transnational activity that orders" cyberspace.[111]

In conjunction with the UN, the United States should lead a multilateral effort to adapt the existing international regime of laws and norms governing warfare to address aggression in cyberspace, or build a new regime for the new warfighting domain. Only the UN has the "membership and capability to address these issues in a meaningful way that will have a global impact" to this global problem.[112] Regulation within individual countries alone will prove ineffective.[113] Already the world has seen "Internet activities considered to be legitimate in one country violate the laws in another."[114]

Additionally, the United States should lead a UN effort to establish an institution to "serve as a clearinghouse and coordination center" to pool international cyber security initiatives and maintain standards.[115] The regime and institution would define international relations within cyberspace and provide a mechanism for the international community to initiate sanctions or punitive actions for noncompliance. The knowledge that a cyber attack is an act of war provoking a severe and costly reprisal from the global community would serve as a strong deterrent to would-be cyber aggressors. The proposal for such a new regime fully supports the U.S. National Security Strategy, in which the President urges, "where existing institutions and regimes can be reformed to meet new challenges, we…must reform them. Where appropriate institutions do not exist, we…must create them."[116]

The Council of Europe's (CoE) Convention on Cybercrime provides the United States with a solid basis on which to build a new international regime. The CoE recognized that addressing the transnational character of cybercrime required a global effort.[117] The treaty fosters international cooperation to fight crime in cyberspace and defines various offenses as cybercrimes with the intent to "establish a common criminal policy," improve deterrence, and "reduce the number of countries in which criminals can avoid prosecution."[118] However, this convention cannot be extended to cyber war as it treats cyber attacks as crimes against private and public property and makes no distinction between the scope and impact of the attack, "thereby disregarding the national security dimension of the threat."[119] Despite these shortcomings, the convention still serves as a model for international cooperation and the development of a larger-scale regime.

The United States is uniquely suited to lead this effort. "The United States…acts as an architect of global and regional security affairs for the purpose of containing new-era dangers."[120] More importantly, this effort allows the United States to shape international norms for state behavior in cyberspace in accordance with American national interests; to do otherwise risks forfeiting this advantage to other nations. For example, China is engaged "in the debate of defining cyber warfare, in part through the Shanghai Cooperation Organization, in order to have a hand in the shaping of a legal framework and rules of engagement related to this new warfare."[121]

To strengthen the new regime's ability to deter cyber attack, the United States should also lead research and development efforts to improve attribution techniques. This includes accelerating ventures like the multilateral effort within the UN to trace original sources of Internet communications and reduce the anonymity of cyberspace; creating an "International Caller-ID capability" of sorts for the Internet.[122] Such an effort "requires multilateral actions that transcend jurisdictions and national boundaries."[123] Ultimately, an acknowledged ability to track aggression is essential to deter future attacks by increasing the probability of reprisal and elevating the costs of resorting to cyber attack.[124]

Cyber attack can cause grave damage to national security and must be treated as an act of war. A robust international regime of laws, norms, and definitions provides the basis for deterrence in cyberspace. The United States is uniquely suited to lead efforts to constrain state behavior in this new global, warfighting domain. The Internet is an "interconnected global network of 600 million users served by 15 million hosts connecting nearly 200 countries."[125] Consequently, cyberspace is the world's nervous system; the control system of modern society. Its protection is an international existential concern that should be addressed with urgency.

Impeding Network Centric Warfare: Commbatant Command Information Technology Support

Colonel David A. Barlow, Ph.D.
United States Army

The different information technology support methods used by the ten United States combatant commands impede network centric operations within the Department of Defense. Network Centric Warfare (NCW) is the method used by the combatant commands to wage war. Information technology is a fundamental enabler of network centric warfare. The ten combatant commands use different methods to provide desktop information technology support to their headquarters staffs. The result is different sets of applications, capabilities, and business processes that impede information sharing between commands and the Department of Defense (DoD), and sometimes between a combatant command and its own components. Information Technology (IT) support at the combatant commands, meant to be a NCW enabler, often fails to support information sharing.

Unimpeded information sharing is a central tenet of network centric warfare.[1,2] The current disjointed IT support methods at the combatant commands impede information sharing within and between the commands. This lack of seamless information sharing does not support NCW, and interferes with the combatant commands' synchronization of the elements of national power. Through examination of several of the IT applications meant to facilitate information sharing, this paper will demonstrate the important role combatant command desktop IT support plays in NCW. The joint, interagency, intergovernmental, and multinational (JIIM) nature of the current and future operational environment impose a huge information sharing requirement on the combatant commands.[3] Developing NCW capabilities to better enable the combatant commands to synchronize the elements of national power will require the DoD to fundamentally change the way in which it provisions IT support at the combatant commands.

This paper addresses secret collateral and below IT support, commonly known as "SIPRNet" (Secret Internet Protocol Router Network) and "NIPRNet" (Non-classified Internet Protocol Router Network) services. The Joint Worldwide Intelligence Communications System (JWICS), while fundamentally an IT system, is provisioned through the Defense Intelligence Agency (DIA). DIA provisions JWICS support separately and distinctly from the organizations that provision collateral IT services at the combatant commands.

This paper examines desktop collateral information technology support to the combatant commands as it pertains to network centric warfare at the theater level. It proposes a single solution provided by a single agency to service all ten combatant commands. It examines the strengths and weaknesses of the current information technology support methodology and the proposed solution. Based on this study, the paper provides strategic recommendations aimed at improving the network centric warfare capabilities across the combatant commands.

Background

The United States combatant commands exist to provide command and control of the broad array of forces and functions that the individual Services and Defense Agencies can provide.[4,5] The doctrinal framework in which the combatant commanders assert their command and control has become NCW.[6]

In its most basic form, NCW seeks to achieve increased agility and effectiveness when compared to industrial age warfare. NCW first requires shared awareness. People and systems normally achieve shared awareness through information sharing. NCW practitioners then leverage this shared awareness to achieve a greater degree of self-synchronization. The emergence of self-synchronizing behavior is the core of the power of NCW, leading directly to increased agility and effectiveness.[7] Within the context of IT support at the combatant commands, self-synchronizing behavior automates many internal and external staff functions, reduces administrative work, improves generation of information from data, and increases staff responsiveness.

This increased staff responsiveness could take the form of faster decision making, more time for conceptual thinking, or a combination of both.

The DoD intends its "plug and play" information infrastructure to tie together all of the information generation and analysis assets that fall under the command and control of the combatant commanders.[8] This infrastructure enables the shared awareness that NCW requires. This same infrastructure serves as the conduit of self-synchronization at all levels. The physical instantiation of the DoD information infrastructure at any particular combatant command headquarters is comprised of a set of information technology (IT) systems and supporting personnel. The IT systems and support that are the subject of this paper comprise the "last mile," quite often literally, of the DoD information infrastructure.

The DoD provisions IT support at the combatant commands through a multi-tiered system, shown in figure 1. The Secretary of Defense, through the Assistant Secretary of Defense Networks and Information Integration (NII)/DoD Chief Information Officer (CIO), determines overall DoD IT policy. The OSD(NII)'s stated mission is to "enable net-centric operations."[9] The Defense Information Systems Agency (DISA)

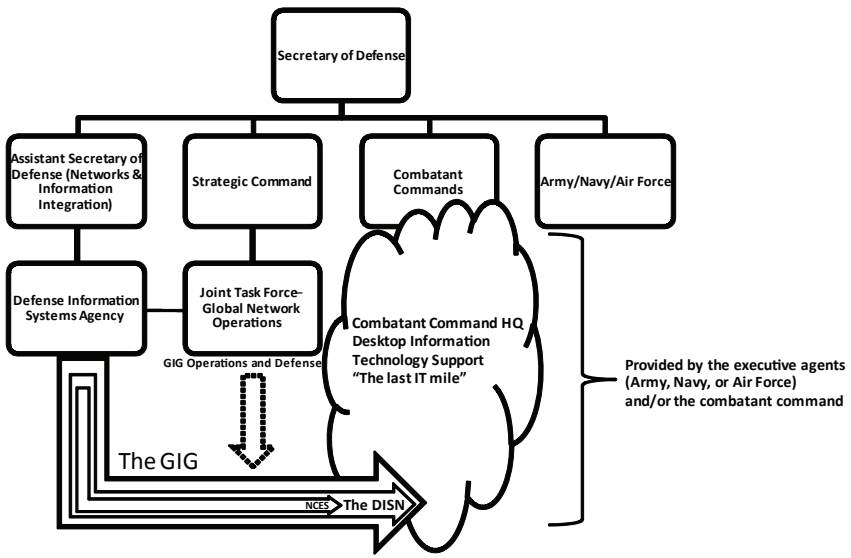

Figure 1: DoD Organization for IT Support at the Combatant Command Headquarters

works for OSD NII and is responsible for the Global Information Grid (GIG), a broad-band telecommunications network and associated services. The GIG is similar in nature to a commercial IT services provider when viewed from a computer networking perspective.

The data transport portion of the GIG is the Defense Information Systems Network (DISN). The GIG/DISN provides "points-of-presence" at various DoD locations, including all combatant commands, for high-speed network services access. DISA funds DISN services through a Defense Working Capital Fund (DWCF), with the Services paying for most of the combatant commands' DISN support.[10] DISA, via the GIG/DISN, provides NCW-enabling enterprise-level software services – collaboration tools – to all DoD network users. DISA calls this program "Network Centric Enterprise Services" (NCES). These NCES replace individual combatant command collaboration tools that have limited or no interoperability and tenuous funding. The NCES tools enable network-centric collaboration across all DoD elements, including the combatant commands. NCES has freed all DoD elements, including the combatant commands, from having to operate and maintain (and fund in many cases) their own fundamentally non-network centric sets of collaboration tools.

Joint Publication 1, *Doctrine for the Armed Forces of the United States*, states that the U.S. Strategic Command (STRATCOM) has responsibility to "plan, integrate, and coordinate DOD global network operations."[11] STRATCOM does so through the Joint Task Force – Global Network Operations (JTF-GNO).[12] The commander of DISA is dual-hatted as the commander of JTF-GNO.[13]

The desktop IT support considered in this paper is the user interface to the GIG; the "last IT mile" between the GIG/DISN and each IT user. This "last IT mile" is extremely important to NCW as much of the information that combatant commands' use is created, manipulated, and stored by the various "last IT mile" systems connecting the GIG/DISN to the combatant commands' desktops.

Desktop IT support at a combatant command headquarters is the purchase, installation, operation, and maintenance of hardware and software systems to support the business processes of that headquarters.

This IT support encompasses all user devices such as the desktop and laptop computers and the software on those computers. It also includes cellular devices and software used to provide mobile email and Internet access. The local network infrastructure is part of desktop IT support. This infrastructure includes server rooms with associated servers and support infrastructure, most software run on the servers in the server room(s), 24x7 help desk services, and the logistics system that supports every IT item, cradle to grave. The level of support required is significant – meeting the 24x7, high-reliability IT requirements of the combatant commander and his staff is an extremely demanding mission. Likewise, the cost is significant – in the neighborhood of $25 million annually per combatant commander when a contractor provides the support.

As a primary enabler of NCW, IT support has become ever more vital to the functioning of the national defense. As computer networking developed in the 1990's, desktop IT support struggled to keep pace, particularly from an organizational perspective. The Services each developed their own methods to provide this support, only modestly unified by the common hardware (IBM-PC architectures), operating system and office productivity software (Microsoft products), and the TCP/IP protocol. In all the Services, desktop IT support started as a small-unit activity. IT systems were not standardized from any perspective. Over time, each Service has adopted a much more centralized approach. The Navy has completely contracted out their desktop IT support to a single contractor. The Army and the Air Force each use a combination of contractors, service personnel, centralized provisioning, and standards to provide their versions of desktop IT support. The Services' motivation for central and standard solutions has been driven much more by lack of resources than enhancing NCW capabilities. However, these central and standard solutions have enhanced the Services' NCW capabilities. From the desktop IT support perspective, these enterprise solutions better enable information sharing and improve the potential for self-synchronization within the Services.

The DoD assigns each combatant command a Service as its executive agent.[14] The Service, as executive agent, has numerous responsibilities, including provisioning of IT support.[15] For each combatant command, the executive agent accomplishes provisioning of IT support unique

to that command, primarily influenced by the executive agent's IT support system. Executive agent control of IT support funding, or lack thereof, has also influenced the wide spectrum of IT support methods employed at the combatant commands.

There are several DoD Directives that deal with information technology.[16] None of the directives specifically address desktop IT support. Their perspective is strategic, yet their direction applies quite specifically to the "tactical" problem of provisioning desktop IT support at the combatant commands' headquarters. Several of these directives address constructing and enabling a network centric DoD. All of them apply direction at the enterprise level, raising but not addressing the question: Is the DoD and Joint Community, comprised mainly of the combatant commands, an "enterprise?" A network-centric approach to warfare would seem to require the answer to be a resounding "yes!" Yet given the current desktop IT support situation, there is certainly not such an enterprise – particularly when it comes to data and information management.

The DoD Directive *Management of DoD Information Resources and Information Technology*, serves as the capstone DoD information system directive. While it does not directly address combatant command IT support, it does direct DoD Components to use DoD-wide automated information systems and software.[17] This Directive, along with DoD Directive "IT Portfolio Management,"[18] require a level of IT management expertise and resources normally found only at organizations providing enterprise-level IT support. These organizations are few within the DoD – DISA, the Services' communications commands, and the Defense Intelligence agency (DIA) are examples.

The DoD Directive "Data Sharing in a Net-Centric Department of Defense," mandates that DoD data be visible, accessible, understandable, and trustable; and by inference, retained for possible future use.[19] The implementing guidance for this directive clearly recognizes the magnitude and difficulty of implementing this mandate, explicitly breaking the implementation into "communities of interest" in an attempt to build this capability incrementally.[20] Additional direction on network centric data conformity, provided by DoD Directive 8320.03,

mandates unique identification (UID) standards for "discrete entities." It infers that each combatant command is such a discrete entity.[21]

Joint doctrine does not directly address the provisioning of desktop IT support to the combatant commands. Joint Publication 6-0, "Joint Communications Systems," does not address combatant command headquarters IT support; the reader is left to infer that it is a combatant command J-6 responsibility.[22] The focus of Joint Pub 6-0 is on force projection communications and network operations, all supported by the GIG.

IT Support Methods

The differences in IT support methods at the ten combatant commands are well illustrated by examining the extremes. On one end of that spectrum is the Navy-provisioned support of Pacific Command (PACOM) and on the other end is the "do-it-ourselves" approach of European Command (EUCOM). The two commands have many similarities. Both are geographic combatant commands (GCC), responsible for engagement with large numbers of countries spread over large geographic areas. Both have assigned forces through their component commands, and both have been in existence since the end of World War II. The executive agent for PACOM is the Navy, while the executive agent for EUCOM is the Army.

The Navy provides IT support to PACOM via the Navy Marine Corps Intranet (NMCI). NMCI is a consolidated, enterprise approach to providing IT support to Navy and Marine Corps forces, activities, and supported commands such as PACOM. At end state, NMCI will support over 700,000 users with standard sets of hardware and software services.[23] NMCI is a multi-year contracted effort costing several billion dollars, and has been the subject of considerable congressional scrutiny. It has suffered from most issues that large enterprise-wide projects tend to incur – particularly projects focused on satisfying the needs of hundreds of thousands of customers.[24] The IT Services Division in the PACOM J6 provides the staff interface between the PACOM staff and NMCI; NMCI staff manages all the IT hardware, software, and network operations. Headquarters PACOM business processes and/or

technical requirements that require changes to the NMCI standardized solution(s) must be implemented in such a way that all NMCI users remain supported and all security requirements remain satisfied. In practice, customization of enterprise IT systems is a difficult task both administratively and technically. Therefore, reaction time to user requirements that necessitate change is usually lengthy. This tends to force organizations to comply with existing network standards rather than pursue solutions that would require network changes.[25]

Although the Army is the executive agent for EUCOM, most of EUCOM's IT support is self-provided. Using an IT services contract provided and managed by the General Services Agency (GSA),[26] EUCOM has a task order that provides all aspects of IT support with the exception of the unclassified network infrastructure – cable, switches and routers provided and managed by the Army. A contractor provides all other IT support through the task order off the GSA contract. All the IT hardware, software, and network operations are managed directly by the Headquarters Enterprise Services Division in the EUCOM J6. Because the IT contractor responds directly to EUCOM's requirements, EUCOM's desktop IT services directly reflect the local requirements of the EUCOM Headquarters staff – i.e. they are customized and often have limited compatibility with components and other combatant command IT systems, from a business process perspective and/or a technical interface perspective.

NCW-Related Problems Created by IT Support Methods

The current combatant command HQ IT support methods significantly impede the NCW tenets of shared awareness and self-synchronization. Fundamentally, the NCW issue is information sharing – it is extremely difficult, if not impossible, for all the required parties to see and use each others' information due to fundamental incompatibilities that the support methodologies introduce into the information technology systems. This section of the paper will examine several examples where systems and/or support methods inhibit rather than empower NCW.

Tasker Management. Tasker management is an excellent example to comprehensively exhibit how the current IT methods inhibit NCW.

The "tasker" is a documented requirement for some kind of work. Tasker systems are used throughout the DoD. Normally, DoD staff elements use taskers for staff actions and not direct command and control of forces. As such, tasker information is sometimes associated with the non-military elements of national power – an important consideration as NCW at the combatant command level must consider and help synchronize all elements of national power.

Taskers drive much of the work that occurs at combatant commands – and the tasker management systems contain much of the information that this work generates. There is a diversity of tasker management systems in use in the combatant commands, as well as the Joint Staff. This diversity has lead to inaccessible information both inside and outside the commands, as well as ad-hoc methods to bridge the systems so that taskers can flow between the Joint Staff and the combatant commands, and between the combatant commands and their component commands. In some cases, this information, when stored in the personal account(s) of a staff member, is destroyed when that staff member departs a command. The impact on NCW is that much of the information generated by the work of combatant commands is excluded from present and future NCW shared awareness efforts, impeding progression to the self-synchronization sought through NCW methods.

For many years, EUCOM has used Microsoft Outlook as the IT software system supporting its tasker management business process. Using this system, little data is accessible beyond the action officer, except for those recipients of the emails generated by the business process. When action officers depart the command, IT management personnel delete their accounts for security reasons – along with all of the information they acquired and generated during their assignments.[27] Personal Outlook files are not publically searchable – so the user can only manually transfer this information by emails and attachments.

As a self-supporting IT services organization, EUCOM developed its own tasker management system. Several years ago, Outlook was a convenient tool that met the business process – NCW was not a factor and the extremely limited information availability was an acceptable risk. For several years, EUCOM has attempted, on its own, to develop,

purchase, and implement other software systems to better support tasker management. To date, these efforts have been unsuccessful due to lack of resources in the Command, most notably government IT persons with business software expertise. The resulting deleterious second order effects of software customization to meet business processes and user training and acceptance have caused Outlook to remain in place, despite its information management and NCW issues.

EUCOM's components all use different tasker management systems. Of note, U.S. Air Force Europe (USAFE) has implemented a specifically tailored Microsoft product for tasker management that provides for information availability to all its users. Africa Command (AFRICOM), derived from and collocated with EUCOM, has chosen to implement this same Microsoft product, tailored to the requirements of AFRICOM. EUCOM has chosen to replace its Outlook-based tasker management system with a government-owned software product originally designed for configuration management. This software has a user interface customized by EUCOM (using a contractor) for tasker management. While all these example commands have taken steps in a positive direction for information management and NCW, none of the tasker management systems are directly compatible, and will require "gluing together" of their respective data-management systems to create the information compatibility required for NCW.

The lack of a single common tasker management system across the DoD, or at least a set of compatible systems across the Joint community, is directly the result of the fractured methods used to deliver desktop IT services. DoD leaves each command to develop its own system – and each does so because it must. The combatant commands might realize a huge savings in staff effort if they had easy and routine access to all their previous work. Yet past work is often inaccessible at best. The "knowledge" foundation required to support shared awareness across the broad spectrum of combatant command work documented by taskers simply does not yet exist – and may not exist until an agency with the right expertise in information management, business enterprise software, and NCW develops and fields a common tasker management system across the Joint community.

TSCMIS. Several of the combatant commands have each developed their own Theater Security Cooperation Management Information Systems (TSCMIS). Each TSCMIS serves as an information focus point for the command's theater security cooperation programs, as well a tool to enhance the command's theater awareness directly supporting command and control. The systems are the combatant commands' major IT link to information supporting the non-military elements of national power. The information contained in these systems is already essential to the shared awareness required by NCW. However, the lack of a single IT services provider for all the combatant commands has caused those who need a TSCMIS system to develop their own. There has been effort at the OSD level to pull the individual combatant commands' TSCMIS development processes together. While a good idea, this has created a competition between the commands for who's system will "win," requiring additional resources to be spent advertising and defending the existing systems. Without any single agency in place to both guide the development and become the program manager (PM), a single TSCMIS solution for all the combatant commands seems unlikely. The resulting system incompatibilities will continue to be an impediment to the seamless information sharing that NCW requires.

Defense Messaging System. The Defense Messaging System (DMS) is an IT system that directly supports DoD-wide command and control (C2). DMS is essential to the combatant command C2 mission. All DMS messages are stored and thus form an historical record of combatant command C2 actions. This information is essential for the shared awareness required by NCW. Unlike standard email messaging, DMS has required delivery times, assured delivery, precedence, as well as security and directory service features tailored to the DoD mission. DISA has overall responsibility for the DMS, but the executive agents usually provide DMS service to the combatant commands. Each Service executes this mission differently, using different user software, and sometimes with indifferent funding priorities. The result is the combatant commands have different user interfaces and different access to the stored messages. More importantly, the combatant commands sometimes find themselves embroiled in funding disputes with their executive agents over the continued financing of this vital

system. When this enormous store of historical C2 data is transformed per DoD Directive 8320.02 to enable NCW data sharing, Service implementation and funding differences will likely not produce the unified results needed by the combatant commands for future NCW development. DMS also has an uncertain future, as DoD has not developed a replacement for this legacy system. If the DoD eliminates DMS without fielding an equivalent replacement, this could force the combatant commands to come up with their own individual solutions. The data and functional incompatibilities this could introduce would be detrimental to future DoD NCW efforts.

Global Command and Control System – Joint. The Global Command and Control System – Joint (GCCS-J) is the DoD Joint Command and Control (C2) enterprise information technology system of record tied most closely with implementing a user interface for NCW at the combatant commands. The DoD uses GCCS-J to correlate and share situational awareness and to monitor, direct, and execute missions. GCCS-J provides operational environment awareness by generating a near real-time picture necessary to conduct joint and multinational operations. The system integrates imagery, intelligence, status of forces, and planning information.[28] DoD fielded the GCCS-J to the combatant commands several years ago, and is currently developing and fielding periodic hardware and software upgrades.

There are several issues associated with local IT support and GCCS-J, a DISA program of record. Maintaining currency in hardware and software; and promoting wide-spread use by combatant command personnel are the two most important issues affecting NCW capabilities. Each combatant command has responsibility for funding most GCCS-J upgrades (with funding from its executive agent); the PM then supports the purchasing, fielding, and training of GCCS-J upgrades in cooperation with the combatant commands desktop IT support process. As funding is almost always in short supply, GCCS-J funding requires prioritized recognition by the combatant commander. GCCS-J is not widely used outside of joint commands; therefore many senior commanders have only cursory knowledge of its capabilities. This makes it difficult for the IT staffs to get GCCS-J upgrades prioritized to achieve reliable and timely funding.

The lack of comfort with GCCS-J on the part of joint senior leadership as well as their staffs has led to limited use of GCCS-J. People tend to use enterprise IT systems that their leadership uses; when leadership avoids or works around an enterprise system, so does the rest of the organization.[29] For GCCS-J, the small user-base means limited user-demand for new or expanded capabilities. The system becomes stove-piped. A single common combatant command IT services provider could better manage the funding and upgrades, as well as promote the use of GCCS-J and other future NCW systems at the user level. Those same users could provide valuable feedback to a single agency where that feedback would affect current and future systems. As it is, combatant command users provide feedback on all IT systems to their local IT services providers, who in most cases have little or no influence over the fielded.

Multi-National Information Systems. The Multi-National Information Systems (MNIS) is a DISA program that provides the Combined Enterprise Regional Information Exchange System (CENTRIXS) and other coalition networking capabilities. DISA globally links the individual combatant command CENTRIXS networks; the combatant commands own and operate their local network elements in virtually the same model as used for NIPRNet and SIPRNet capabilities. However, the CENTRIXS set of hardware and software is relatively limited and standardized so in theory, the data issues for NCW are far fewer than in the U.S.-only IT services discussed above. However, the tenuous year-to-year funding of the combatant command CENTRIX networks combined with the different forms of desktop IT support have created a static technology and user training situation. This effectively prevents any network(s)-wide improvements in NCW capabilities, such as the data sharing technique required by the DoD Directive "Data Sharing in a Net-Centric Department of Defense."[30]

Senior Leader Decisions. Combatant commands, in particular the geographic combatant commands, tend to be current operations-focused and have tightly constrained resources. Therefore, senior leadership decisions that impact desktop IT support within these commands will almost always give priority to the current operations requirements over long-term requirements such as implementing

NCW-capable systems. Users generally view desktop IT support as a utility, much like electric power and telephone service. This could be a suitable model if IT support was regulated and provisioned like other utilities – regulated by DoD to international standards and provisioned by large, independent providers such as the Services and/or DISA. However, desktop IT support at the combatant commands is neither regulated (with the exception of security) nor independently provisioned. In all dimensions, with some security exceptions, it responds to the requirements of the combatant command. The combatant commands' focus on current operations, most especially in the geographic combatant commands, makes it extremely difficult for them to support long-term NCW-enabling efforts.

Possible Solutions and Analysis

The solution space for supporting NCW through combatant commands' desktop IT support is fairly well constrained. A consistent constraint is the level of classification – Secret – and therefore the requirement for heavy involvement of U.S. government personnel and U.S. security clearances for most IT support personnel. The current desktop IT support solution is a diverse, evolutionary set of different support structures. It represents the least centralized, most locally-controlled overall solution. The most centralized solution would be for a single DoD Agency, most logically DISA, to provide centrally-managed desktop IT support for all the combatant commands. In the middle of this solution space would be the different IT support structures presently in place, with additional oversight and program management from JTF-GNO and DISA. These three points in the solution space are analyzed in detail below, with a focus on meeting the need to support NCW through desktop IT support at the combatant commands.

There are three major areas to examine when comparing and contrasting these three possible solutions. The first is the most critical – does the solution continue to support ongoing combatant command operations at least as well as the present solution? The second: does the solution significantly improve the future NCW capabilities of the supported command, inclusive of the JIIM environment, and the DoD? Finally,

what resources and bureaucratic changes will the DoD have to make to implement the solution?

The status quo has managed to provide suitable desktop IT support to conduct current operations. As discussed previously in this paper, the status quo does not support NCW in a suitable manner, failing most particularly in the management of data and information, and the adoption of NCW-focused systems. In fact, it places the future of NCW in the combatant commands in peril. For that reason alone, it is not a suitable solution for the future of desktop IT support at the combatant commands. However, the current set of IT solutions does provide some significant advantages to some of the combatant commands, i.e. local control of both IT resources and the funding that buys and supports those IT resources. As this solution is also the current solution, changes to resourcing or bureaucratic systems are not required.

A solution that increases the oversight of DISA and JTF-GNO to control the separate combatant command desktop IT support systems could significantly improve the future of NCW in the combatant commands. This solution builds on the DoD IT support model already in place, in which JTF-GNO provides a significant level of network control focused on security, and DISA provides program management of a few DoD IT systems-of-record (e.g. GCCS-J and MNIS), some web-based DoD-wide NCW-enabling collaboration tools, as well as support and assistance with network security systems. This solution could improve the future of NCW IT systems within the combatant commands if it is able to overcome the significant resistance to "new and improved" that IT users exhibit when asked to give up their "tried and true" solutions. The major obstacles are choice and often the overwhelming current operations focus of some of the commands. The local IT support ownership of some of the combatant commands gives them an option; if they do not like the DISA-provided solution, they can keep or seek their own. Stovepipe solutions do not support NCW within DoD or in the JIIM environment. Those commands with Service-provisioned solutions face the opposition of the Services to adapt their Service-oriented IT systems to include what are typically Joint-only solutions. Adaptation almost always costs resources. This solution does take

advantage of existing resource and bureaucratic systems. However, it would require additional resourcing of JTF-GNO, DISA, and the combatant commands' IT services. Tighter control and additional PM work automatically incurs additional resource costs, with no offsetting savings. In addition, compliance with additional control and additional PM fieldings will require additional work by the IT support services at the combatant commands, again with no offsetting savings.

Handing over responsibility for all combatant command desktop IT support to DISA is not as radical a solution as might first appear. Presently, DISA provides DISN services to each of the combatant commands. Each combatant command has a supporting DISA field office. In terms of IT, the DISN brings high-capacity SIPRnet and NIPRnet connections from the Global Information Grid (GIG) to the combatant command desktop IT systems. DISA also provides some PM services, some web-based DoD-wide NCW-enabling collaboration tools (NCES) as well as a significant level of assistance via training, inspections, systems, and exercise support in the network security arena. Giving DISA responsibility for all elements of the combatant commands' IT support is the logical next step to strongly bolstering the future of NCW in the combatant commands and the DoD. It removes the most significant obstacle to IT systems that enable NCW at the combatant commands, mainly the reluctance and inability of the combatant commands to pull their own resources away from the current operations mission to support future IT systems development and fielding.

An Example of Success

A DoD agency already successfully provides a service to all the combatant commands – and part of this successful service provisioning includes desktop IT support. The Defense Intelligence Agency (DIA) provides the Joint Worldwide Intelligence Communications System (JWICS) to each combatant command as part of an overall intelligence support package.[31] This IT support includes hardware, software, and DIA personnel and contractors to provide desktop support, plus future systems development, fielding, and training. DIA supports the combatant commands' intelligence IT completely, enabling the

commands to focus their intelligence resources on their missions, rather than partially on intelligence IT support. This DIA JWICS support model, applied to collateral IT support, could strongly enhance NCW from a technology perspective. As a pure information services agency, DISA could bring much more expertise to the problem of improving desktop IT technology to support NCW than the one or two persons at each combatant command who might have this task as an additional duty; DISA could also bring more expertise to bear than any of the Services. A DISA solution follows the existing "chain-of-command" for NCW IT solutions. OSD/NII has the mission of enabling network-centric operations. The commander of DISA works for the Assistant Secretary of Defense, NII. DISA is already responsible within DoD for providing network-centric enterprise services – with the exception of the "last IT mile" to the desktops of the combatant commands. That "last IT mile" is absolutely critical to maximizing the NCW capabilities of the combatant commands.

Recommendations

1. DISA should prepare to assume responsibilities for desktop IT support to the combatant commands.
2. DISA should quickly assume support of the combatant commands' coalition desktop IT services as part of its MNIS program. The CENTRIX networks present an opportunity for DISA to assume a well-defined but small portion of desktop IT support duties for the combatant commands. As a test case, this should provide DISA and the DoD with the experience needed to eventually assume all combatant command desktop IT support.
3. DISA and combatant command representatives should study the DIA model used for providing intelligence support to the combatant commands. Where appropriate, DISA should analyze the experiences gained by DIA and adapt and adopt these experiences to support desktop IT support at the combatant commands. This study group must place special emphasis on supporting NCW.
4. DoD should extract the additional resources required by DISA from the existing desktop IT support structures at the combatant commands. This includes personnel and funding. DISA could

adapt the Defense Working Capital Fund approach to include future costs of providing desktop IT support to the combatant commands, enabling baseline IT service costs to continue to be funded by the Services (as the combatant command executive agents), with optional and/or enhanced desktop IT support services to be funded by the requiring combatant command(s).

Conclusion

This paper has discussed desktop IT support at the combatant commands and its effect on NCW capabilities. With specific focus on information sharing as an enabler of the NCW tenet of self-synchronization, this paper examined several examples of current combatant command IT systems. It also examined the effects of combatant command senior leader decisions regarding IT support to current operations versus modernization to support DoD-wide NCW capabilities. The research revealed that the current desktop IT support methods do not adequately support combatant command NCW capabilities. After examining three possible future combatant command desktop IT support methods, this paper provided the recommendation, with supporting discussion, that DISA become the single provider of desktop IT support to all the combatant commands.

Knowledge Centric Warfare: An Introduction

Lieutenant Colonel Robert B. Sofge
United States Marine Corps

On 15 January 2009, the Chairman of the Joint Chiefs of Staff (CJCS) published his Capstone Concept for Joint Operations, calling it the most fundamental of all U.S. military concepts.[1] In it, Admiral Mullen describes a vision for the future joint force in terms of four military activities: combat, security, engagement, and relief and reconstruction. He lauds U.S. forces today as the most capable in our nation's history. However, after praising people as our greatest advantage, he states that our patriotism, training, discipline, leadership, and ability to adapt are not enough to meet future challenges. Somehow, something is missing.

Missing are new capabilities and improved capacities of existing ones as well as doctrine, tactics, techniques, and procedures. The CJCS advocates new methods of integration, as well as better selection, education, training, equipment, and management of the force – led by broadly educated, adaptive, and thinking professionals to meet the full spectrum of national security challenges. Beyond the professional commitment and honor imbued in the current force, we must cultivate the all-important ability to take proper action in the absence of specific guidance.[2]

The Chairman offers 17 institutional implications for the joint force to fulfill his vision. Eight of these call for direct more coherent development of knowledge and adaptability within our force:[3]

- Improve knowledge of and capabilities for waging irregular warfare.
- Improve knowledge of and capabilities for nuclear warfare and operations in chemical, biological, and radiological nuclear environments.
- Improve knowledge of and capabilities for security, engagement, and relief and reconstruction activities.

- Markedly increase language and cultural capabilities and capacities.
- Institute mechanisms to prepare general-purpose forces quickly for new mission sets.
- Improve organizational solutions for protracted missions that cut across geographical boundaries.
- Develop innovative and adaptive leaders down to the lowest level.
- Improve Service and institutional adaptability to deal with rapid change.

The Chairman's imperatives signal both a shift of focus within, and expansion of, the military domain from today's framework of Network Centric Warfare (NCW) toward what Phister and Plonish call Knowledge Centric Warfare (KCW).[4] At first this appears to be a simple evolutionary step from the centricity of the 1980's platforms and the 1990's networks to the future centricity of knowledge.[5] But it is also a profound shift back to what has been most important all along – the physical and mental capacity and capability of our Soldiers, Sailors, Airman and Marines, as well as that of the professionals supporting them.

The shift is timely and appropriate because the threat has changed. Instead of operating within the effective and clearly defined Westphalian concept of political and military competition between states, we now do battle with conditions. Although U.S. and coalition military might is unrivaled, the elusive nature of our collective political objectives is frustrating. Fortunately, in improving each warrior's understanding of the broad range of the tools of war and techniques for the local or national application of the instruments of power, we become more effective. By integrating knowledge itself more thoroughly into the force, we create the capability to be successful not only in a war against people, but also in a war among the people.[6]

This paper proposes a more careful focus for the collective joint force to support the Chairman's vision. It proposes a knowledge-centric framework for understanding the complex nature of warfare at all levels. It suggests that the necessary evolutionary step that will capture the promises as well as fill the voids within NCW resides in

centering our warfighting ontology on the people who fight wars and what they know – and not the technology supporting them. This thesis is overtly philosophical since knowledge resides in humans who know – living, breathing, understanding, and fallible, but potentially brilliant, people who are central to any enterprise. This thesis presents an epistemological challenge to those who misunderstand the subtle but enormous difference between knowledge and information, which is born of the gradual corruption of what it means to know.

Due to the tremendous gains in our capacity to store, process, and manipulate information in the modern age, many people now mistake the capture of data and information, however contextually rich, as the preservation and distribution of knowledge. Accordingly, knowledge centricity is a response to the dilemma that while we swim in information, we are starving for knowledge.

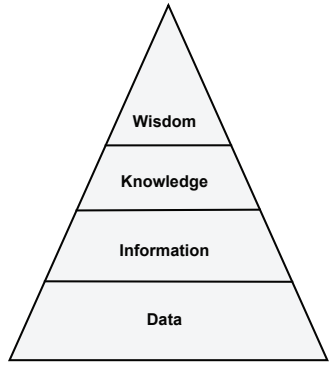

Figure 1: The Knowledge Pyramid

KCW takes the best of the network-centric operational concepts to the next level. It culls the proven ideological tenants from those less viable and, with focus on the warrior, applies all we have learned. In 1998, the introduction of NCW revolutionized the way both warriors and thinkers view war, yet this concept remains somehow incomplete. The complex, intricate, and awe-inspiring technological marvels of silicone and steel we have created do not capture what Clausewitz called the passion of war. KCW focuses on what we know and how we know it – on what is in our minds and how it got there. It is knowledge of ourselves and the enemy in a broader, more integrated context, creating a knowledge edge by "leveraging and exploiting information, communications and other technologies, and by the application of human cognition, reasoning and innovation."[7] Knowledge Centric Warfare, empowered by technology, embraces the fundamentals of Knowledge Management (KM) to generate an advantage by influencing decision-making and enhancing effective execution.[8] KCW centers on the warfighter, developing then synthesizing the mental acumen and technical savvy

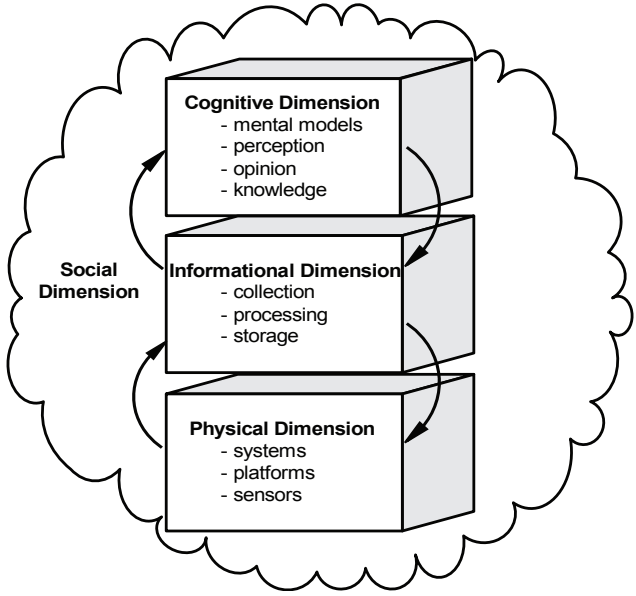

Figure 2: The Information Environment[9]

required to fulfill the Chairman's vision while developing a collectively superior force.

KCW, like KM, is an integrative concept – it attempts to reassemble our perception of the world in some semblance of how it "really" is by beaming its messages at the intersection of people, process, and technology. The ambiguity of the "information age" environment initially fostered the development of Information Technology (IT) solutions to KM with the vague promise that organizational commitment, zeal, and money might transform the seeking firm into the vaunted "learning organization."

The notion that KM can be purchased from a software vendor and deployed by an institution initially blurred the KM picture by emphasizing the wrong node of KM's process-people-technology triad. Current research in the quest to manage knowledge is shifting institutional focus away from primarily IT solutions to a more integrated, people-centric view, thereby relegating technology to a supporting role, though one still essential. The organizational imperative of knowledge transfer is now assuming a more social character in the form of Communities of Practice and other IT enabled forums.

Similarly, KCW is a broad, abstract concept centering at the intersection of our technological capacity, the processes embedded within our war-fighting apparatus, and, most importantly, the people using both to prevail in the modern struggle of wills. In Power to the Edge: Command, Control in the Information Age, the authors discuss four dimensions of command and control (C2): physical, informational, cognitive, and social (see figure 2).[10]

Physically, NCW connects platform sensors and systems into a cohesive whole. At the information level, data is pulled, posted, processed, and stored.[11] Often overlooked (or assumed) is the cognitive development of the people using these systems and sensors as well as the social domain in which they operate. KCW emphasizes the cognitive and social domains of not only C2, but also the nature of warfare itself.

Philosophical Roots: Epistemology, Semiotics, and Cognition

What is knowledge? This is certainly a question for the ages, and one that philosophers, scientists, poets, religious leaders, and the rest of the world's great thinkers have struggled with for recorded history. Indeed, one's answer to this question frames one's approach to many things, but a workable answer is a core component of KCW. Fortunately, by standing on the shoulders of the great thinkers of our time, it is possible to develop at least a working definition of what knowledge is for the purposes of creating the KCW framework.

Epistemology, from the Greek word episteme, meaning "knowledge," is a branch of philosophy that considers the nature, origin, and limits of human knowledge and understanding.[12] Among the ancient philosophers, both Plato's theory of forms and Aristotle's examination of cause and effect holds that knowledge is possible when subjected to reason and logic. Conversely, ancient skepticism, like that of Pyrrho, is a philosophy of doubt that generally suspends judgment on our capacity to know anything and holds that true knowledge is impossible, masked by appearances and sensory misperception.[13]

Modern (17th-19th century) philosophers and epistemologists – Descartes, Locke, Hume, and Kant among them – pondered the true

nature of knowledge and set rigorous standards for what constituted actual knowledge as opposed to some lesser form of intellectual activity. Two principle schools of thought emerged: rationalism, which posits that certain a priori knowledge exists in the mind; and empiricism, which asserts that all knowledge is experiential.[14] Though rooted in more ancient philosophy, John Locke's "blank slate" is a modern expression of empiricism.[15] Famously, Descartes' *Cogito Ergo Sum*, or "I think, therefore I am," is a skeptical philosophic proof. After careful examination, he determined all of his previous knowledge was simply belief when subjected to his standard that all knowledge is certain cognition and certainty is freedom from doubt. The only irrefutable claim to knowledge he could make was that because he could think, he must exist, and his existence was therefore true.[16]

Kant, inter alia, distinguished knowledge from opinion and faith by theorizing about levels of ascent, where each level is subject to increasingly stringent justification. At the lowest level, a knower can hold a proposition weakly supported by reasoning – an opinion. More stringent, but still subjective beliefs are assents held strongly, but they lack objective sufficiency. Knowledge, the final rung, is "assent that is sufficient both subjectively and objectively."[17] Clearly, Kant's classifications rely on their sufficiency – needing some form of internal or external justification to cross the thresholds of propositional ascension.

Using a proposition construct for the consideration of what constitutes knowledge, the claim to having knowledge of a given proposition requires three things: truth, belief, and justification, each "individually necessary and jointly sufficient"[18] to support the epistemological claim. As such, the Justified True Belief (JTB) construct is a model for knowledge (where p is the proposition and K is the knower) generally given as:[19]

S knows that *p* if and only if:

p is true;[20]

K believes that *p*;

K is justified in believing *p* (either internally or externally).[21]

Prominently, the philosophic pursuit of Truth, solidly in the realm of epistemology, exceeds the scope of this paper. But the acceptance of JTB as a working definition for knowledge, however contingent or tentative, is sufficient to the extent that knowledge inextricably requires a knower. Of the several challenges remaining, those of utmost concern are: discovery of how knowledge manifests itself within an organization; methods of capturing, reusing, and generating knowledge; and techniques of representing knowledge.

Cognition

Cognition is the process or act of knowing, inclusive of perception and judgment. It is the experience of knowing, as opposed to feeling or willing.[22] Cognitive science is a relatively new interdisciplinary field embracing "philosophy, psychology, artificial intelligence, neuroscience, linguistics, and anthropology"[23] Arguably, cognitive awareness is the sine qua non of knowledge and is the threshold for distinguishing knowledge from otherwise contextually rich information.

Semiotics

> *All instruction is either about things or about signs; but things are learned by means of signs.*[24]
>
> —Augustine (On Christian Doctrine, I:2).

Semiotics is a branch of philosophy that concerns itself with signification and language, particularly as it relates to the concepts or things that signs (sounds or symbols) represent. It is important because it has everything to do with how we convey elements of what we know. The capacity to accurately convey and interpret meaning both within and beyond organizational bounds poses a significant challenge, even as we use a "common" language to explicate data and information. In an increasingly globalized world, changing languages while preserving meaning is a tremendous informatics challenge. Brodner asserts that semiotic challenges are the principle reason "most real IT implementations have turned out to be a barrier to rather than an enabler for organizing more productive work and value creation processes."[25]

Broadly, semiotics is broken into three categories: semantics, syntax, and pragmatics.

Semantics is the study of meaning within language best illustrated by an old joke that highlights different meanings of the word "secure" within the U.S. Armed Forces:

Commander: "Secure that building!"

- A Sailor immediately turns out the lights and locks the doors.
- A Soldier posts an MP and no one gets in without a special pass.
- A Marine sets up machine gun crossfire, lays down a mortar barrage, and calls for air strikes and artillery support.
- An Airman takes out a two-year lease with an option to buy.

Given the same command, each audience interprets it differently and acts accordingly based on the cultural model to which they subscribe. Discussion of cultural models follows.

Syntax concerns itself with the formal use of rules and standards for combining symbols to convey meaning. Proper grammatical structures for the writer and logical precision for the computer programmer are examples of syntax, which effectively conveys the intended meaning or instruction through the application of specific rules.

Pragmatics involves the study of conveying more meaning than that which is explicitly stated. Inference is required on the receiving end of a pragmatic statement to derive the fullest meaning. A moment of reflection might reveal that most misunderstandings between people are the product of pragmatic misfires. Pragmatism requires more than context – it requires a priori knowledge (but not in the Kantian sense) and is sensitive to not only what is said or written, but also to what is not.[26]

Shared meaning reduces semiotic challenges within groups. Developing a shared lexicon is a critical component in the development of shared meaning, especially across organizational boundaries. Beyond shared meaning, understanding how knowledge flows within an organization and how shared meaning becomes a shared understanding is important.

In Dynamic Theory of Organizational Knowledge Creation, Nonaka cautions "although the terms 'information' and 'knowledge' are often used interchangeably, there is a clear distinction between information and knowledge."[27] He then quotes Dretske:

> *Information is that commodity capable of yielding knowledge, and what information a signal carries is what we can learn from it. Knowledge is identified with information-produced (or sustained) belief, but the information a person receives is relative to what he or she already knows about the possibilities at the source.*[28]

Organizational Learning and Knowledge Transfer

There are three general approaches to knowledge transfer within organizations: the positivist approach in which objects have independent meaning in the world; the social-constructionist view that assumes knowledge is a social construction whose meaning derived from its usage; and the socio-cognitive perspective that assumes knowledge is internalized in the mind and body of the knower and then reconciled through external influences. The validity of the accepted approach depends on the philosophical notion of what constitutes knowledge which, in turn, determines the threshold that information must cross to become knowledge.

Nonaka posited there are two types of knowledge: tacit and explicit. He theorizes knowledge is created, or transferred, through the conversion of the two types.[29] Tacit knowledge is the knowledge inside one's head, and explicit knowledge is tacit knowledge somehow externalized, recorded in some way to facilitate its disembodied transfer. Nonaka further identifies four modes of knowledge conversion between the two types (See figure 3, next page):[30]

- Tacit-to-tacit: Occurs between people thru face-to-face socialization – shared experience, observation, imitation, and practice.
- Explicit-to-explicit: Between individuals thru some medium: phone, email, etc.
- Tacit-to-explicit: Externalization of knowledge – recording what you know.

- Explicit-to-tacit: Similar to traditional learning, internalization of disemodied knowledge.

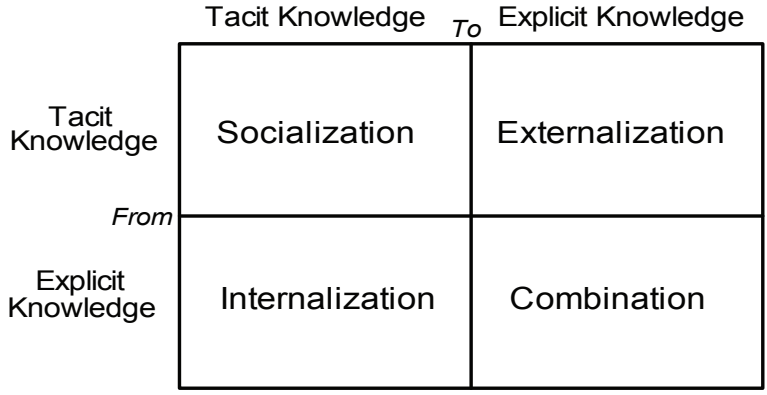

Figure 3: Nonaka's Model of Knowledge Transfer

Nonaka's model exhibits significant explanatory power, but is subject to misinterpretation if not considered in his full context. Specifically, the interplay between the tacit and explicit knowledge involves a cycle that creates or transfers knowledge through at least one iteration. Contributing to the confusion, Nonaka himself uses explicit knowledge and information interchangeably in his discussion of explicit-to-explicit, or the combination knowledge transfer mode: "The reconfiguring of existing information through the sorting, adding, recategorizing, and recontextualizing of explicit knowledge can lead to new knowledge."[31] This objectification of knowledge, disembodied from the knower as a type on intellectual currency, has allowed terms like "knowledge-base" to replace "data-base" in our evolving lexicon and undermines what it means to know.

The positivist approach to knowledge transfer assumes that disembodied knowledge can be stored and its meaning adequately codified to qualify as knowledge.[32] The principal challenge associated with a positivist perspective is the assumption that a retriever will be able to interpret, in context, the captured knowledge.

The social-constructionist approach to knowledge transfer, built upon constructivist theory, posits derivation of meaning comes through usage. Constructivists assert individuals construct knowledge for themselves in context of the physical world around them while building

on knowledge previously acquired. Immanuel Kant, Jean Piaget, and Lev Vygotsky are among important contributors to the constructivist theory.[33] Vanden,[34] cited in Lauzon, asserts, "learning is a constructive process in which the learner is building an internal representation of knowledge, a personal interpretation of experience…an active process in which meaning is developed based on experience."[35]

Situated Cognition is a subset or branch of constructivism developed by Lave. It asserts that while knowledge is acquired through the context of activity, knowledge transfers take place only in a similar situation, and they are largely unintentional.[36] The condition of a similar context is the underpinning of Communities of Practice,[37] or forums of similar experience. Similarity of experience and context enables the transfer of knowledge.[38]

Etienne Wenger and Jean Lave first introduced the term Communities of Practice (CoP) more than 15 years ago.[39] In a later work, Wenger, et al., define CoP as "groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis."[40] The authors assert that while the term is relatively new, the idea of a community of practice is quite old. They cite medieval guilds as an early example, and believe the concept retains the capacity to create a framework and infrastructure in a modern learning organization.[41]

The shift in thinking from a KM perspective is important as it moves away from viewing knowledge as an object or artifact. This is a tendency of IT-dominated KM efforts that focus on codification and capture. As a result, data, information, and knowledge are culled from their context in a tacit-to-explicit knowledge transfer process, and thus lose meaning. This tendency is affirmed in a 2004 case study of a Danish software firm where "management's preoccupation with implementing technological solutions for codifying, archiving, and creating global access to information [was] conflicting with the practitioners' focus on seeking context-rich information through collegial networks."[42]

Instead, in a connectionist view of knowledge, in which the knower is a required entity and the separation of the knower from the known is impractical (if not philosophically impossible), CoPs create a

vehicle for sharing tacit knowledge. Nonaka believes that the majority of organizational knowledge is tacit, embodied in the people that comprise the organization.[43] CoPs create and exploit the social and cultural underpinnings of knowledge by facilitating tacit-to-tacit knowledge transfer.[44] The largest store of organizational knowledge may be tapped by creating conditions conducive to the transfer of elusive and difficult-to-capture tacit knowledge.[45] So, it is not difficult to understand the broad appeal of a Communities of Practice approach to managing and creating organizational knowledge. CoPs are effective because the shared cultural models upon which they are based facilitate the transfer of information, thereby creating knowledge.

Structure, Design, and Membership of a Community of Practice (CoP)

CoPs can take many forms; they are typically organized around common goals. They can be sponsored by an organization or exist outside any formal recognition.[46] In either case according to Wenger, a CoP shares three fundamental characteristics: a domain of knowledge, a collection of people concerned with the domain, and a shared practice.[47] Practice is the operative word; it is the engine that drives negotiation within the community. Practice fosters sharing of knowledge and best practices by those who are actually engaged in the CoP. The practicing community ultimately discovers new knowledge.

Wenger offers seven conditions upon which a CoP should be designed "with a light hand": the ability to evolve, open dialogue among varying perspectives, different levels of participation, both public and private spaces, a focus on value, a balance between familiarity and excitement, and rhythm.[48] Within this fluid design, Dalkir,[49] citing Kim, breaks community membership into five categories – visitors, novices, regulars, leaders, and elders – each beginning with different levels of participation that potentially mature through participation.[50] An example would be a visitor who becomes a novice participant because the visitor found value in participating. Through exposure, time, and participation, the individual could evolve into a leader within the CoP.

Fisher's 2004 study on CoP within the Data Management User Technology (DMUT) Division at the IBM Corporation expands Wenger's three fundamentals of a CoP while adopting them in a more formal fashion. Abandoning the light-handed approach, Fisher stresses the important role of common goals and missions within the IBM communities.[51] The purpose of the formalized goals and missions directed by management, as opposed to Wenger's more ad hoc approach, is to provide a rally point for the diverse and cross-functional members of the communities within the division. Each knowledge domain centers on a product group and communities fall into two distinct categories: skill-based communities and goal-based communities. Employees typically belong to at least one community of each type and can belong to more than one group in a skill-based CoP.[52]

At IBM's DMUT, the skill-based CoPs function much as Wenger describes. Workers with a common skill set share best practices in an informal, collaborative environment. Fisher specified four mechanisms adopted at IBM for the nurturing of these skill communities: skill-based councils sponsored by companies whose members form the CoP; collaborative communication and learning facilitated by both the company intranet and Lotus Notes to transfer knowledge and document best practices; mentorship, which closely observes Kim's model; and physical proximity, a deliberate attempt to collocate knowledge workers close to their skill-based communities.[53]

Goal-based communities perform a different function at DMUT. More aligned with traditional western corporate hierarchy, these communities form among specific product groups and their membership is multidisciplinary. They focus on the product; producing it on time and within budget. The goal-based communities interact with each other and govern the skill-based communities. Firmly grounded in corporate reality, Fisher notes that "the skill communities do not exist to exhibit perfection in their skills; they exist to contribute those skills to a specific business-related goal, such as the design, development, and shipment of Product A on schedule on budget."[54]

This valuable case study describes one way to establishment CoPs in a large corporation and offers a concrete example of CoPs in action.

Fisher concludes by describing the struggle to find balance between the different types of CoPs at IBM – perfecting skills as well as creating and sharing knowledge versus the business imperatives of schedule and budget. The study does not offer any metrics to assess the value added by the CoPs.

For all their utility, CoPs do not offer a complete KM solution in industry, nor are they the panacea for KCW. While there are enthusiastic sponsors of the concept and a growing body of literature on CoPs, actually measuring the CoP contribution to business enterprise remains difficult. If it cannot be measured, how has it managed to create a competitive advantage?[55] In a farming analogy, practitioners are encouraged to plow a fertile field in the proper place hoping for a viable yield; however, this "faith-based" approach is not an option when the security of the nation is at stake. Other models and theories of learning have applicable explanatory power in the knowledge transfer process (See Table 1).[56] Additionally, within CoPs themselves, undisclosed issues that could limit their viability are lurking in dark corners.

The social dynamic within a CoP is left to nature in much literature. Roberts allows that issues of power, trust, and predisposition are powerful influences in the community. The development of shared meaning within the community might simply reflect the dominance of powerful community members. Issues of trust, based on a host of sociological factors, can inhibit sharing of knowledge. Likewise, members' predispositions regarding participation might limit the degree to which the CoP is a viable solution in certain environments.

Hemre describes the importance of recognizing CoP life cycles and their relative values over time.[57] Wenger offers caution regarding the dual-edged nature of CoPs: "shared perspectives on a domain, trust, a communal identity, longstanding relationships, and an established practice – are the same qualities that can hold it hostage to its history and its achievements."[58] Communities might become atrophied by certain historical best practices and immobilized in the community power structure. These circumstances could inhibit the creativity and innovation that was their charter. In view of the power of doctrine, such obstacles to a dynamic CoP could be debilitating.

Theory	Principal Authors	Key Points	Model
Problem Based Learning	Barrows and Kelson	Hands on active learning Investigation and resolution of messy, real-world problems	Cultural
Experiential learning	Kolb	Four stage cycle Combines experience, perception, cognition, and behavior	Cultural
Affordance Theory	Gibson	World is a perception and perception drives action	Private
GOMS Model	Card, Moran, and Newell	Human information processing Predictive behavior in uncertain situations	Private
Discovery Learning	Bruner	Inquiry based instruction Best for learners to discover facts and relationships	Private
Situated Learning	Lave	Learning is unintentional Role of activity, context, and culture	Cultural
Stage Theory of Cognitive Development	Piaget	Cognition develops in four stages: sensorimotor, preoperational, concrete, and formal	Private
Multiple Intelligences Theory	Gardner	Seven ways people understand the world: Linguistic, Logical-Mathematical, Visual-Spatial, Body-Kinesthetic, Musical-Rhythmic, Interpersonal, Intrapersonal	Cultural

Table 1: Learning Theories

The principal contribution to the development of KM and to KCW by the CoP approach is the departure from principally technological solutions toward sociological considerations in the construction of learning organizations. Their reliance on the social nature of learning and knowledge transfer brings rich context to the KCW triad. Whereas technological contributions receive much emphasis and lean six-sigma initiatives aggressively study processes, the CoP concept brings the same level of attention to understanding the most important component of knowledge and its management – the people.

A more complex and powerful socio-cognitive approach to knowledge transfer reveals the profound impact of mental models on individual cognitive processes, somewhat in contrast to the social constructionists' emphasis on shared practice and experience.[59] Cultural and private mental models create an interpretive framework for socio-cultural feedback and strategic thinking processes (categorical and reflective

thinking). The implication is that nuanced interpretation is a prerequisite to knowledge. Further, the cognitive interplay of the relative strength of cultural and mental models explains how the same data applied to the same scenario by different people often leads to different knowledge outcomes. It follows that the objectification of knowledge upon which both the positivist and social constructionist approach to knowledge transfer rely is too simplistic.[60] To understand the creation and transfer of knowledge one must account for cognitive processes and the factors that influence them. Ringberg and Reihlen offer a four-step recursive process:[61]

- Cognitive context: embodied cultural and private models
- Cognitive content: reflective/categorical/strategic processing
- Environmental feedback: divergent-convergent social processes
- Cognitive outcome: collective, negotiated, unique, or stereotypical knowledge

The cognitive outcome or knowledge this process produces using the socio-cognitive model offers a great deal of flexibility and better reflects real-world observed phenomena.

Negotiated knowledge emerges from discrepancies between the mental models of the participants. It is typical of cross-boundary information exchange between practitioners of different disciplines who hold different assumptions.[62] However, the exchange remains valuable only as long as the participants remain engaged and they dissect, understand, and ultimately resolve their discrepancies. Resolution constitutes an adjustment in the participants' cultural or private models and it forms the basis for more effective knowledge transfer in the future (see figure 4).[63]

Collective knowledge relies on shared cultural models that come from shared experience, education, or training – items that are typical in military organizations.[64] It relies less on reflective thinking and more on categorical thinking. Knowledge transfer in this scenario is akin to the silent hand and arm signals shared among infantryman, produced by intense training to develop shared cultural models. More personally, it is the power of "the look" between a husband and wife, emanating

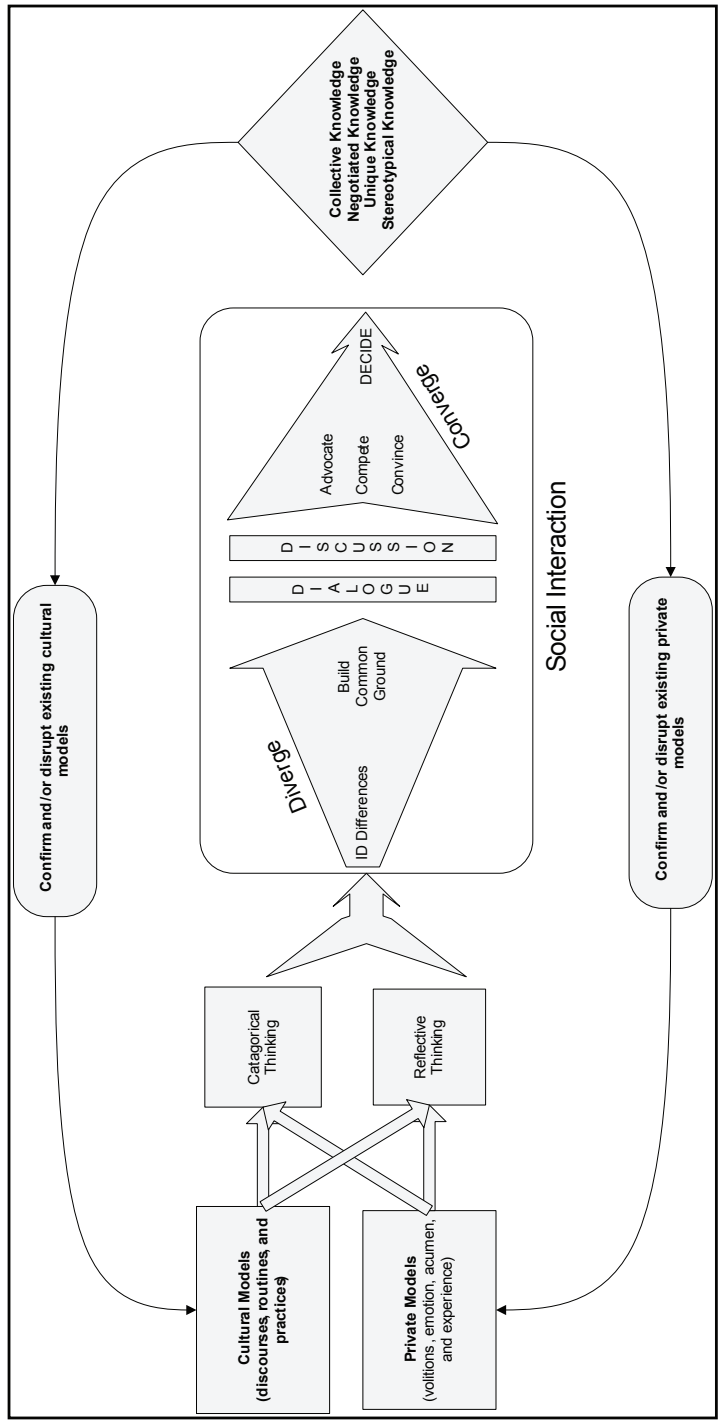

Figure 4: Cognitive Outcomes on Knowledge Transfer (adapted from Ringberg and Reihlen)

from the shared traditions, customs and habits developed through an intense personal relationship. One of the challenges of this type of knowledge is that it limits knowledge transfer from those outside the group. Empirically, a glimpse of the challenges among the military branches, services, and the interagency support this concept.

The remaining two knowledge transfer scenarios relate to the degree of categorical thinking or reflective thinking involved. Unique knowledge embeds a high degree of reflection, with limited social interaction and little categorical influence.[65] Self-created conceptual worlds dominate the cognitive capacity of those with unique knowledge. The transfer of unique knowledge is rarer due to limited social interaction of what Ringberg and Reihlen call an emancipated postmodernist disposition. However, often those with unique knowledge are able to contribute disproportionately to out-of-the-box thinking that is perhaps foreign to categorical thinkers, provided a social bridge connects the two.66

Stereotypical knowledge refers to transfer scenarios where categorical thinking dominates with little evident reflection. Routines for the sake of the routine, which are characteristic of large bureaucracies, are a typical manifestation of stereotypical knowledge.[67] Without reflection, stereotypical knowledge may lead to blind spots or cognitive comfort in situations that should be alarming.

Adopting a more complex view of knowledge creation and transfer, where private and cultural models are of critical importance for the generation and identification of the four types of knowledge, is a key step in the evolution of KCW. Additionally, the active development of private and cultural mental models held by each of us (applying relevant aspects of the learning theories introduced Table 1.) is of paramount importance.

Toward the Centricity of Knowledge

This paper offers theoretical justification to alter the philosophical aim point in the development of the future force. Our professional development should focus on the cognitive capacity of those who populate our networks, as opposed to the technical capacity of the network itself. This shift will enable us to build a force more capable

of embracing the full spectrum of traditional and emergent military responsibilities. This cognitive development, in turn, requires deliberate focus on developing the mental and cultural models inherent in everyone. Evolving from NCW to KCW requires a reexamination of the assumptions upon which NCW rests.

David Alberts describes NCW as having four basic tenets. First, a robustly networked force shares information more readily. Second, sharing information both increases the quality of the information shared and facilitates collaboration. Third, shared awareness is the result of greater collaboration and leads to self-synchronization. Finally, taken together, the previous three tenants dramatically improve mission effectiveness.[68] This analysis assumes that when connections have been established, they will be used to achieve effective ends. Implicitly, NCW assumes connected people will collaborate to generate new levels of knowledge because they are connected.

At the heart of NCW is Metcalf's law. Introduced by George Gilder in 1993 in an article about Metcalf's observations, the law states that the value of a network is proportional to the square of its users.[69] In the case of NCW, this value is roughly analogous to warfighting capacity. It follows that more nodes equal more combat power. Additionally, Alberts asserts that network-centric operations apply to more than just high-intensity, force-on-force warfare. He claims networks create the potential, albeit subtly, to be successful in irregular warfare when applied appropriately.[70]

However, we are really using all of the networks to create knowledge in the minds of the human beings. Thus, we should focus on the cognitive dispositions of our force through a deliberate effort to create the conditions that give rise to new knowledge.[71] A more viable assumption is that technical capability will continue to increase due to the global nature of computing in the information age. It is more effective to develop our minds using existing networks, social and technical, to generate a warfighting advantage.

The modularization of warfighting organizations into smaller and self-contained fighting enterprises empowered by the ability to share information represents a move away from industrial age organizational

theory.[72] The older and more rigid C2 mechanisms have yielded grudgingly to flatter and more efficient structures. In the newer construct, the demand for strategic knowledge at the tactical level compels development of intellectual adroitness across the force. The ubiquitous nature of information flow in modern society respects neither linear nor vertical lines of communication. The premise of the "strategic corporal" whose real-time tactical actions have strategic consequences relegates the formal chain of command to nothing more than simply another actor on the national security stage.[73]

Private mental and shared cultural models perform the sense-making function in cognition. Taken together, they form the multifaceted lens through which we view the world. KCW, specifically categorical thinking is the point of leverage.

The deliberate development of reflective thinking is another useful lever. Strategic thinking is not the exclusive territory of national strategists. Strategy, or the artful application of ends, ways and means to achieve national security, can be used at any level in an organization -- the end can be local or global. The socio-cognitive model of knowledge transfer provides a method to understand the impact of mental model development and the resultant types of knowledge produced. Fortunately, a renewed KM effort is underway. If it is properly applied, it may provide the strategic advantage necessary to accelerate the evolution of the force and realize the CJCS's vision.

Knowledge Management in the U.S. Army

The Army first recognized KM in 2001, emphasizing the IT demands of the emerging concept in vogue at the time. More recently, the Army published Field Manual (FM) 6-01.1, *Army Knowledge Management* (AKM), a doctrine that advances, develops, and articulates 12 principles largely adapted from the civilian sector (see figure 5).[74]

"It's all about increasing collaboration, and that has huge implications for war fighters," according to Bob Neilson, KM adviser to the Army's CIO. "It's about not only sharing information but having the responsibility to provide knowledge across the enterprise."[75] FM 6-01.1 relies heavily on Nonaka's theories of knowledge types and transfer

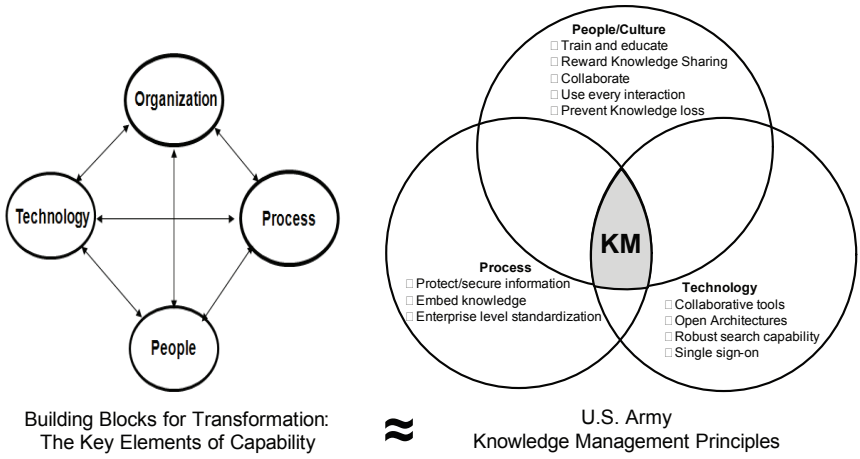

Figure 5: Transformation and KM Principles

processes.[76] Consequently, there remains mixed messages regarding what constitutes information as opposed to knowledge as well as critical semantic difference. However, the document is a significant step forward because it establishes structure and functions for a KM staff in support of commanders.

Conclusion

Although a compelling factor in warfare through the ages, technology itself is but one factor accounting for the superiority of one force over another. Currently, among the dominant technologies are the computer networks born of the information age. Although this burgeoning technology can capture and store information, as well as process and deliver information at the limits of imagination by means of vast arrays of granularity and concise summation, it does not create knowledge. The analysis and synthesis leading to genuine understanding is irrevocably a mental process. As such, increasing the usefulness of the networks, both socially and technologically, must depend ultimately on the development of the cognitive capacity of those who use them.

KCW lies at the intersection of people, processes, and technology. This composite concept crosses academic and organization boundaries by definition. KWC focuses on developing knowledgeable warfighting professionals – what they know, how they know it, why they believe it,

where they learned it, and how that knowledge enables others. KCW facilitates enterprise-level thinking in an effort to achieve strategic synergy at the joint and interagency level.

Just as NCW built upon Platform Centric Warfare, KCW will build upon NCW – a logical, more refined, and powerful concept that focuses on using the tools rather than building them. The focus of NCW has been to build, protect, and populate the net. The focus of KCW is use the net to develop and protect the knowledge, and thus know the net thoroughly.[77] KCW is about warfighters and their capacity to know.

The true strength of a knowledge centric approach is it its intrinsic ability to prepare warriors for the unexpected. In Inevitable Surprises, Peter Schwartz advises that while we will be surprised in the future, we can be in a position to deal with it by increasing our ability to both see opportunity and respond to surprise. He admonishes readers to place "very, very high premium on learning" while noting that most failures to adapt are in fact failures to learn quickly enough.[78] KCW creates a framework that enables us to learn quickly enough to respond vigorously to the inevitable surprise, and thus protect the nation.

Enabling Security, Stability, Transition and Reconstruction Operations through Knowledge Management

Commander Timothy L. Daniels
United States Navy

The challenges inherent in today's strategic environment amplify the criticality for adaptive and responsive leadership and organizations. Globalization and rapidly diffused information flows tighten global interconnectedness and create the expectation for near instantaneous and decisive action. Strategic leaders face demands for effective and timely analysis and decision-making that juxtapose a host of ill-structured or wicked problems.[1] These unique, crosscutting, and interactively complex problems often require perpetual sets of neither correct nor incorrect cascading solutions. Additionally, leaders and organizations face an external environment characterized as volatile, complex, uncertain and ambiguous (VCUA).[2] It is an environment requiring innovation, accelerated transformation, pervasive sensing and continual learning. In essence, tumultuousness prevails. The VCUA environment drives rapid external and internal change, decision and resource demands, and evolving missions and strategic foci as leaders and organizations attempt to shape, influence, adapt and respond.

The post-conflict Security, Stability, Transition, and Reconstruction (SSTR) efforts in Iraq and Afghanistan typify strategic operations in tumultuous and VCUA external environments.[3] Compounding the substantive challenges inherent in this environment, however, is an equally complex internal environment comprised of multiple organizations collectively responsible for the SSTR mission. As outlined in *National Security Presidential Directive-44* (NSPD-44), the Secretary of State has overall responsibility for coordinating, leading and integrating U.S. SSTR efforts across all "U.S. Departments and Agencies with relevant capabilities" and also those of the nation's coalition partners.[4] Specific to the United States alone and although dependent on the situation, these organizations may encompass the Departments

of Defense, Treasury, Energy, Agriculture, Commerce, Health and Human Services, Transportation, and Homeland Security, among others. Accomplishing the SSTR mission, thus, requires collaboration, coordination, synchronization, and synthesized execution across an extremely complex network of responsible organizations with differing values, cultures, norms, technologies, policies and goals. Additionally, in-theater organizations characterized by discontinuous membership exacerbate internal challenges through inconsistent ebbs and flows of information, situational awareness, and, most importantly, experience-derived knowledge.[5] Collectively, this complex multi-organizational construct must effectively address a myriad of SSTR requirements and wicked problems that transcend organizational hierarchies and authorities.[6]

Addressing ill-structured or wicked problems in the context of SSTR efforts requires that the network of responsible organizations build sufficient collaborative and SSTR-specific long-term problem solving capacity.[7] Building this capacity, in turn, necessitates that leaders and organizations within the network create, acquire or draw upon, and add to a collective SSTR knowledge base through learning. Learning occurs by attempting to structure or address SSTR problems; namely, the "designing" cognitive function of operational art.[8] Learning also occurs by assessing decision or solution implementation and adjusting based on outcomes. Overall, however, the complex problems themselves often become "the main objects to be dealt with and the driving force behind knowledge acquisition."[9] A growing knowledge base, thus, is critical to generating new ideas and fostering innovation and creativity required to address or structure other, emerging, or future SSTR problems. In essence, the knowledge created or acquired through addressing SSTR wicked problems becomes the very resource required to continue effectively doing so.

The efforts by the United States and Coalition partners in Iraq and Afghanistan clearly demonstrate that collaboration, organizational learning, and knowledge sharing are essential elements of post-conflict Security, Stability, Transition, and Reconstruction Operations (SSTRO. Specifically, knowledge created and shared within and among responsible organizations enables timely and effective problem

solving, decision-making, adaptivity and responsiveness critical to successful SSTRO in VCUA post-conflict environments. As such, Knowledge Management (KM) provides a key strategic SSTRO enabler. Organizational culture, however, poses a major barrier to effective knowledge management employment within and across the U.S. Department of Defense (DOD) and interagency organizations.

The analysis provided herein explores KM as a strategic SSTRO enabler and specifically examines the efforts of the Combined Security Transition Command-Afghanistan (CSTC-A) using the Intelligent Complex Adaptive System (ICAS) Model of KM. The ICAS model describes how KM creates the organizational intelligence necessary for effective and efficient response to the environments characteristic of SSTRO. Accordingly, applying the ICAS model demonstrates the strategic utility of KM for SSTRO-tasked DOD and interagency organizations. Implementing KM to achieve strategic success, however, necessitates overcoming prohibitive cultural barriers. Considering this, the analysis provided herein also explores organizational culture as a barrier to KM implementation and use and includes focus areas for overcoming culture-centric obstacles. Finally, the analysis concludes with three recommendations centered on realizing the strategic utility of KM as part of SSTRO and in achieving national security objectives overall.

Analytical Precursors – Learning Organizations and Organizational Knowledge

Successfully accomplishing the SSTR mission necessitates unity of action and effort. The multi-organizational network must effectively function as a whole in addressing SSTR challenges presented by the external VCUA environment, as well as the wicked problems inherent in the overall SSTR mission. An integral component in achieving this strategic end-state is to establish an internal environment that has the capability and capacity to do so. This is largely possible given three organizational mandates. First, organizations within the network must value collective knowledge creation, sharing, acquisition, and application. Second, organizations within the network must understand how their actions affect both the external and internal environments.

Finally, organizations within the network must not only recognize requirements for change, but also have the capacity to effectively and intelligently change based on internal and external drivers. In this context, two critical enabling concepts emerge, specifically Learning Organizations and KM. Although the focus of this analysis is on KM as a strategic SSTRO enabler, Learning Organizations and KM are synergistic and mutually supportive.[10] Further, Learning Organizations posses or develop a culture of learning, which is a knowledge-centric endeavor, and organizational culture is a significant determiner of KM success.[11] As such, briefly exploring certain key aspects of Learning Organizations as an enabling component of the internal SSTRO environment, as well as KM success, provides a worthwhile backdrop for the follow-on KM analysis herein.

Harvard Business School professor David Garvin (1998) defines a learning organization as "an organization skilled at creating, acquiring, and transferring knowledge, and at modifying its behavior to reflect new knowledge and insights."[12]

In the context of SSTRO and KM, developing a network of learning organizations will help create the required internal environment previously described from three perspectives. First, learning organizations are knowledge-centric and value the creation and sharing of knowledge; learning becomes an important aspect of the overall organizational culture, which, in turn, affects effective KM implementation and use.[13] Second, learning organizations utilize a systems thinking approach to understand decision and action implications.[14] Organizational and network knowledge is an essential component of systems thinking as it assists in understanding complexity and recognizing high-leverage change.[15] Accordingly, a system thinking focus has the potential to improve decision-making. Finally, learning organizations seek to adapt or change, including organizational behavior or structure if required, based on the effectiveness of their actions.[16] Faced with an external VCUA environment, adaptivity and agility increase organizational effectiveness and responsiveness. In a complex internal environment, adaptivity and agility better position organizations to embrace change, such as that associated with KM implementation and use.

Exploring KM as a strategic enabler for SSTRO also requires understanding the concept of knowledge in organizations. Thomas Davenport and Laurence Prusak (1998) define knowledge as follows:

> *Knowledge is a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information. It originates and is applied in the minds of knowers. In organizations, it often becomes embedded not only in documents or repositories but also in organizational routines, processes, practices, and norms.*[17]

There is an intuitive understanding that knowledge goes beyond data and information – a type of hierarchy or continuum that builds or moves from data to information to knowledge. Data represents "discrete, objective facts about events."[18] Although organizationally valuable, data by itself has no meaning. Conversely, adding meaning or value to data, through contextualization, categorization, calculation, correction, and/or condensation, transforms data into information.[19] Information provides increased organizational value over data, and organizations invest heavily in processes and technology tools dedicated to information management. Similar to information, knowledge has meaning, but despite frequent interchangeable use, information and knowledge are not the same. Unlike information, knowledge "is about beliefs and commitment" and "is a function of a particular stance, perspective, or intention."[20] Also unlike information, knowledge is closer to action; the final intellectual asset required for planning or implementing solutions to problems.[21]

Organizationally, knowledge tacitly or explicitly derives from information through individuals or groups as either a manageable process or asset.[22] Tacit knowledge, which has both technical and cognitive dimensions, is personal, contextual, non-tangible, or typically within the mind of the knower such as "know-how," mental models, heuristics, intuition, innate intelligence or the ability to reason.[23] Tacit knowledge predominantly derives from experience and practice, and is a resource that improves the speed and effectiveness of decision-making and problem solving. Explicit knowledge, on the other hand, is systematic, formal and something expressible, capable of codification, or documentable in some form of media.[24] Tacit and

explicit knowledge, however, do not exist as separate or discreet entities within organizations. According to pioneering experts within the field of organizational knowledge, Ikujiro Nonaka and Hirotaka Takeuchi, tacit and explicit knowledge interact, known as organizational knowledge creation, through four modes of "knowledge conversion" referred to as Socialization (tacit to tacit), Externalization (tacit to explicit), Combination (explicit to explicit), and Internalization (explicit to tacit) – the SECI model.[25]

Knowledge Management as a Strategic Enabler

Increasingly over the past decade, the concept and practice of Knowledge Management as a mechanism to improve organizational performance pervades organizational literature and focus.[26] In general, KM encompasses the "capture and/or creation, sharing and dissemination, and acquisition and application" of knowledge.[27] Practitioners view knowledge as an increasingly valuable in-tangible commodity due, in large part, to pioneering works by authors such as Peter Drucker who, in 1993, introduced knowledge and the "knowledge worker" as the "basic economic resource" of society.[28] However, a majority of KM research, investment and application generally occurs within the private sector (one exception being the U.S. military) where the value of KM includes increased innovativeness, better decision-making, reduced costs, and faster responsiveness.[29] Today, the private sector predominantly views KM as critical to increasing the "capacity to integrate and apply distributed knowledge to create agility, responsiveness, and adaptivity" in a complex and uncertain business environment.[30] It is a business environment characterized by the geographically unconstrained transfer and exchange of capital, products, services, information, and knowledge throughout a global network of independent and interdependent firms, enterprises, and consumers. Within the private sector, thus, KM delivers a sustainable competitive advantage critical to meeting the demands and challenges of an interconnected, complex and uncertain globalized business environment.[31]

Contextually, the strategic value of KM within the public sector parallels that of the private sector albeit not profit or competition-driven. Explicit and tacit knowledge within the public sector is equally,

if not more, important as public sector organizations are primarily knowledge-intensive.[32] As such, numerous public sector organizations were early to adopt and continue to leverage KM as a strategic enabler. Many U.S. federal agencies, such as the DOD, have well established KM technologies, tools and programs geared toward managing a vast array of data and information.[33] One of the most recognized in KM literature is the U.S. Army's After Action Review (AAR) and Center for Army Lessons Learned (CALL) programs.[34] Leveraging the success and effectiveness of CALL and other programs, the Army is increasing its focus on KM. In July 2008, the Chief of Staff and Secretary of the Army jointly issued a memorandum promulgating the Army's 12 Knowledge Management Principles as a "first step" toward developing an "enterprise approach" to KM from the "cultural, process change, and technical" perspectives.[35] Other well-recognized programs within DOD include the U.S. military knowledge portals, such as Army Knowledge Online (AKO), Navy Knowledge Online (NKO), and Defense Knowledge Online (DKO), that provide information, communication, collaboration, decision support, education, and training environments for a globally distributed workforce.[36] In addition to portals, the U.S. military is leveraging KM communities of practice to increase collaboration, build expertise, expedite information flow, and improve decision-making and problem solving.[37] The Air Force Material Command (AFMC) pioneered KM within the Air Force (AF) promoting communities of practice as a "key technique across the AF."[38] These DOD uses of KM are by no means comprehensive and represent only a few examples. Overall, DOD KM techniques, tools, and practices span a full range of functions including acquisition, intelligence, logistics, and operations with current and future trends moving toward Joint and "cross-service integration."[39]

Within the U.S. public sector, the horrific terrorist attacks of September 11, 2001, represent the most poignant lesson in the criticality of government KM and coordinated action.[40] The lessons learned from these attacks resulted in President George W. Bush establishing the Department of Homeland Security (DHS) to rectify critical knowledge sharing and coordination gaps.[41] More recently, KM is receiving a renewed national security and interagency strategic focus as lessons emerge from the significant security and stability challenges faced in

Iraq and Afghanistan. An April 2008 RAND SSTR study regarding U.S. civilian personnel identifies KM as a critical component for driving "continuous performance improvement by identifying and addressing gaps in effective leadership and implementing and maintaining programs that capture organizational knowledge and promote learning."[42] Additionally, in November 2008 the Project on National Security Reform identified "enhancing knowledge management across all components of the national security system" as a core reform.[43] As evidenced by the relatively recent focus on KM at the national strategic level, KM is receiving increasing recognition as a strategic enabler across the spectrum of U.S. public sector activities.

Aside from the military element of national power, within the public sector realm there is a primary focus on addressing or managing social or public problems, characterized as wicked, where knowledge is integral to structuring or understanding these problems.[44] Specific to SSTRO, the problem sets faced by the multi-organizational network represent the full spectrum of public issues including political, economic, infrastructure, informational, social, humanitarian, and legal, often within societies marked by fledgling governance and reduced security. Regarding the security and stability aspects of SSTRO, U.S. Army doctrine recognizes KM as "key to understanding and exists to help commanders make informed, timely decisions despite the complexity inherent in stability operations."[45] A specific, present day manifestation is the focus Multi-National Corps-Iraq (MNC-I) is placing on KM as a critical enabling capability for operations in Iraq.[46] However, the multi-organizational network responsible for SSTRO, which in many regards is similar to the complex networks found in the global business environment, must synergize efforts and actions across the spectrum of SSTRO given the wicked nature of problems faced. As such and given the spectrum of problems, KM use and focus must transcend only certain departments or organizations to the whole of U.S. government with SSTR capabilities and responsibilities.[47] As articulated by the Chairman of the Joint Chiefs of Staff, even the success of future military operations "will require the integrated application of all the instruments of national power."[48] Derived tactical, operational, and strategic tacit and explicit knowledge within the SSTR network, thus, become critical dynamic strategic resources that SSTR organizations and the network

as a whole must manage. It is the accumulated, largely tacit knowledge that enables the expanding, shared SSTR knowledge base necessary for continuous collective learning, increased problem solving capacity, and improved responsiveness, adaptability, and decision-making.

Managing SSTRO knowledge as a resource within the multi-organizational network, however, presents three primary challenges. These challenges, though, are also the primary justifications for KM as a strategic enabler. First, tacit knowledge is difficult to capture, share, and if possible, make explicit; doing so takes focus and resources and is subject to individual and organizational cultural and social dynamics.[49] However, the knowledge transfer speed and effectiveness required for responsiveness, adaptability and agility in complex and uncertain environments requires rapid and effective knowledge transfer and sharing.[50] Rapid transfer and sharing must include both tacit and explicit knowledge, but realizing this strategic capability is significantly easier with explicit knowledge. Second, in a discontinuous member multi-organizational environment, individual tacit and explicit knowledge ebbs and flows as individuals rotate in and out of organizational positions within the network. Continually expanding and accessing the collective network's knowledge, however, improves problem solving capacity, responsiveness, and decision-making.[51] Finally, leveraging SSTRO capabilities from multiple, globally located organizations results in geographical and organizational knowledge dispersion. Further, organizations within the responsible network vary in technologies, size, structure, cultural values, policies and procedures.[52] Effectively addressing SSTRO challenges and achieving unity of action and effort, however, requires effective knowledge sharing and collaboration throughout the multi-organizational network. In this overall context, despite the significant challenges to KM implementation and use, KM represents a powerful strategic enabler for meeting the demands and challenges of SSTRO in a VCUA environment.

CSTC-A and the Intelligent Complex Adaptive System (ICAS) KM Model

Overall, the mission of the Combined Security Transition Command-Afghanistan (CSTC-A) is to "plan, program and implement

structural, organizational, institutional and management reforms of the Afghanistan National Security Forces (ANSF)" in partnership with the Government of the Islamic Republic of Afghanistan and the international community.[53] CSTC-A accomplishes its SSTRO mission through advisors, mentors and trainers to the Afghan Ministries of Defense and Interior, as well as an internal staff to manage the planning and programming efforts required to organize, man, train, equip, and build facilities for the ANSF. As a United States Central Command (USCENTCOM) organization, CSTC-A must coordinate its efforts with the NATO-led International Security Assistance Force (ISAF) and the U.S. Embassy.[54] Understanding this, collaboration and knowledge sharing are essential to CSTC-A mission accomplishment.

Key components of the CSTC-A SSTRO mission are planning and programming for ANSF generation including manning, equipping, and building facilities. Shared responsibilities necessitate synchronization across U.S. and ISAF organizations to effectively train, field, and equip Afghan National Army (ANA) units and Afghan National Police (ANP) forces. Component members of the CSTC-A staff primarily accomplish assigned tasks through direct internal interaction with other members of the staff, as well as direct external interaction with corresponding component members of ISAF and other U.S. organizations. Equipping the ANSF, for example, requires internal interaction between CSTC-A CJ7, CJ4, CJ8, CJ-Engineering, the CSTC-A Deputy Commanding Generals for ANA and ANP development, the CSTC-A Deputy Commanding General, and the CSTC-A Commanding General. Externally, ANSF equipping requires interactions with staff members from the ANA and ANP, Afghan Ministries of Defense and Interior, ISAF, the Defense Security Cooperation Agency (DSCA), U.S. Army G8, and USCENTCOM J4. Equipping the ANSF also requires periodic external interactions with the DOD Inspector General and the U.S. Congress Government Accountability Office (GAO) as part of their accountability and oversight functions. Due to the VCUA environment associated with SSTRO, the duration and extent of interactions is extremely dynamic and often varies depending on internally and externally driven changes to goals, policies, priorities, and strategic focus.

Viewed through a KM lens, the description of CSTC-A within its strategic and operational environment mirrors that of an Intelligent Complex Adaptive System (ICAS).[55] As such, the ICAS KM model is useful in identifying the criticality of KM within the CSTC-A construct and specifically by using the five key processes within the model of "understanding, creating new ideas, solving problems, making decisions, and taking actions to achieve desired results."[56] CSTC-A performs these processes through continuously evolving interaction with key organizations and stakeholders. For example, CSTC-A purchases ANSF equipment through the DSCA and associated U.S. military service organizations as part of the Foreign Military Sales (FMS) program. As part of the CSTC-A CJ-4 equipping mission, an equipment procurement "sub-system" forms to address the full range of related activities. These activities include requirements definition (understanding); identifying alternatives when specific equipment is unavailable or delivery schedules do not support operational and strategic requirements (creating new ideas and problem solving); signing Memorandums of Agreement (MOAs) based on equipment types and quantities being purchased (making decisions); and executing and monitoring contracts and delivery schedules (taking actions to achieve desired results). Shared knowledge is central to these processes as it represents the critical organizational or network resource that enables effective action in dynamic, complex and uncertain environments.[57]

The equipping example described above represents one of many CSTC-A sub-systems formed to ensure mission accomplishment. However, using the ICAS KM model describes the adaptive nature of CSTC-A as staff "sub-systems" dynamically form and evolve to address SSTRO problems or issues. Internal and external organizational cooperation and collaboration are essential to achieving unity of action and effort. Among the challenges, however, is knowledge attenuation as members of the CSTC-A staff, as well as other organizations, frequently rotate in and out of these sub-systems due to U.S. and coalition military deployment cycles, which can range from six to 15 months, or civilian position transfers. Knowledge attenuation significantly affects organizational effectiveness when key individuals or leaders within the sub-system ineffectively transfer critical experience-based knowledge to follow-on members. Knowledge "vacuums" are frequent as new

members acquire or create sufficient knowledge to add value to sub-system efforts and performance.

The ICAS KM model also identifies eight organizational characteristics useful in analyzing CSTC-A through a KM lens. As depicted in figure 1, these characteristics, which emerge from the nature of the organization, include organizational intelligence, shared purpose, selectivity, optimum complexity, permeable boundaries, knowledge centricity, flow, and multidimensionality.[58] Overall, these characteristics describe how flexibly an organization, within its environment, applies the right knowledge at the right time to attain goals.[59] Within the ICAS model and specific to CSTC-A, these characteristics manifest through hierarchical and sub-system interactions that facilitate vertical internal knowledge flows and external horizontal knowledge flows throughout all levels of the organization. Further, information technology tools such as e-mail, video teleconferencing, shared portals, and meetings enable these knowledge flows and communicate goals, strategic and operational direction, and priorities. Additional enablers

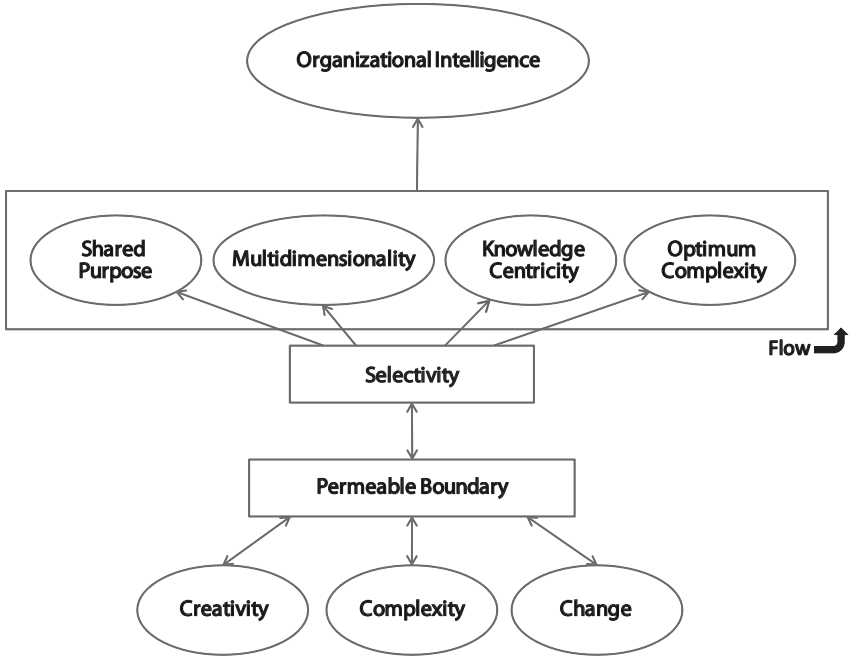

Figure 1: Overview of the ICAS Model[60]

include training, personnel skill alignment, and organizational agility critical to effectively responding to the dynamic external and internal environments. Overall, the ICAS model describes CSTC-A knowledge management through its capacity and ability to solve complex problems as well as make and implement decisions to achieve operational and strategic goals.[61]

Socio-Cultural Implications for Knowledge Management

The "first generation" of KM, which evolved to roughly the mid-1990s, neglected much of the socio-cultural aspects of knowledge.[62] Two studies completed in the late 1990s identified culture as one of the main barriers to KM implementation.[63] During this first generation, KM efforts largely concentrated on information technology and "converting tacit to explicit knowledge" that was more easily shared through information systems.[64] Consequently, despite significant codification and technology investments, ineffectiveness and failure characterized many KM endeavors. Over the past decade, however, the second-, third-, or "next-generation" of KM study and practice increasingly focus on socio-cultural aspects of KM as organizational knowledge derives from people and is subject to group and social dynamics such as organizational culture.[65] These dynamics significantly increase in complexity with multi-organizational networks and contextually, the introduction of Complex Adaptive Systems and Chaos theories in later generation KM models proves instrumental in understanding the role of KM in organizations.[66] However, organizational culture remains a key determinant to KM success as it affects the spectrum of knowledge "capture and/or creation, sharing and dissemination, and acquisition and application" activities.[67]

Organizational knowledge is primarily tacit and as such requires individual willingness to share and the ability to effectively articulate or transfer what is in individual minds.[68] Further, tacit knowledge is more prevalent in increasingly complex environments and problems.[69] Considering that tacit knowledge sharing is the basis for organizational knowledge creation, the social interaction that enables tacit knowledge sharing becomes critical.[70] Organizational cultures and subcultures serve

as a governing mechanisms for this interaction and are key components of "ensuring that critical knowledge and information flow within an organization."[71] Culture dynamically manifests in how organizations value trust, openness, internal and external knowledge, change, innovation, learning, and collaboration. Trust is fundamental to internal and external knowledge sharing and can significantly influence the extent to which individuals are willing to share knowledge.[72] Captured knowledge, ideas, collaboration, and learning contribute to and enhance knowledge creation, sharing, acquisition and application by increasing organizational memory, absorptive and problem solving capacities, and innovation.[73] By extension, culture is often a critical enabler to improved organizational performance in complex environments. Culture also affects the effectiveness of multi-organizational network environments across the dimensions of relationships, accessibility, experience, language, values, and interests.[74] Contextually, thus, organizational culture is an essential element of KM yet often presents significant barriers to effective KM implementation and use.

Overcoming Cultural Barriers

Although cultural barriers to KM efforts cover a broad spectrum, three primary categories emerge. The first category is barriers to knowledge sharing and includes trust, collaboration, social capital, and language. The second category is barriers to knowledge acquisition and includes learning, receptiveness, and absorptive capacity. The third category is barriers to application and includes organizational risk aversion and intolerance. Due to the nature of knowledge in organizations, these categories are not discreet and significantly influence one another. Further, all of these cultural barriers exist to lesser or more degrees within and across the U.S. DOD and interagency environment. Given that organizational culture is the "medium in which organizations reside," changing culture is both a difficult and lengthy process.[75] Implementing and using KM, however, invariably necessitates cultural change. Resultantly, resistance is inevitable and presents an obstacle or block to effective or successful change.[76] Resistance occurs from both individuals and groups which makes addressing resistance challenging.[77] If unaddressed, however, resistance can derail a change effort and may result in the unintended consequences of negative organizational

turmoil, employee dissatisfaction, or the necessity to refocus a change effort toward damage control vice successfully implementing the required change. As such, understanding and overcoming resistance must be an integral part of any KM organizational change strategy.

Overall, the cultural barriers to knowledge sharing center on knowledge creation and capture. The primary barrier to knowledge sharing is lack of trust.[78] Trust develops and improves through social interaction, which is the basis for knowledge creation. Accordingly, organizational cultures that limit or discourage social interaction jeopardize knowledge creation and, by extension, knowledge management initiatives overall.[79] Collaboration, or the extent to which organizations leverage combinative intellectual efforts in achieving goals, also affects knowledge sharing and includes the organizational components of epistemology and identity.[80] Epistemology refers to the "nature" and perspective of knowledge within an organization or network – either objectivist (i.e., knowledge as an object, valuing explicit over tacit) or practice-based (i.e., knowledge as embedded in practice and socially constructed).[81] Organizations with an objectivist perspective tend not to value the social interaction and communication critical to collaboration and knowledge sharing.[82] Additionally, identity refers to the extent to which the organization or network share a sense of purpose or direction.[83] Lacking a shared identity decreases the likelihood of knowledge sharing, which is essential to effective collaboration.[84] Related to collaboration, social capital is "the stock of relationships, context, trust, and norms that enable knowledge sharing behavior."[85] These relationships often are contingent on internal and external politics as well as perceptions of knowledge as a source of power, which can erode organizational trust and, thus, knowledge sharing.[86] Finally, language encompasses the technologies, vocabularies, and mental models or "frames of reference" within organizations.[87] Differences in technologies, vocabularies, and underlying assumptions limit the effectiveness of communication and knowledge sharing; however, these differences typically exist within organizations and across multi-organizational networks.

The barriers to knowledge acquisition center on understanding, or contextualizing, knowledge relative to the knowledge needs of the organization or network.[88] Individual and organizational learning is

inherent in knowledge acquisition and is critical to expanding the capacity of organizations or networks to understand and recognize knowledge deficiencies, obsolescence, and opportunities in addressing or solving problems.[89] Organizational cultures that inhibit learning also limit the capacity of organizations to adapt, develop, and change based on experience-derived knowledge.[90] A second cultural barrier to knowledge acquisition is the lack receptiveness to internally and externally generated ideas, such as a "not-invented here syndrome."[91] Organization cultures characterized by a lack of receptiveness significantly limit how organizations contextualize new knowledge relative to their organization as well as implement change based on lessons learned and in response to environmental demands.[92] The final cultural barrier to knowledge acquisition is low or lacking absorptive capacity within organizations. Absorptive capacity, or openness to change and innovation, relates to existing internal and external knowledge and determines how effectively organizations understand and leverage knowledge as a mechanism for successful change.[93] Organization cultures that do not value openness, learning, or innovation lack in absorptive capacity and are ineffectual in the change required for effective KM implementation and use.

Finally, the barriers to application focus on how organizations use or apply knowledge in decision-making, problem solving, or change efforts. The first cultural barrier to knowledge application is risk aversion. Risk-averse organizations are reluctant to embrace environmental uncertainty and the innovation and creativity required to adapt in achieving desired results.[94] Risk-averse organizational cultures are also less likely to value or apply unproven knowledge as part of decision-making or problem solving processes. Further, risk aversion determines the degree to which organizational leaders will undergo change.[95] The more risk averse the organizational culture, the lesser the degree of change organizational leaders are willing to undergo.[96] The final cultural barrier to knowledge application is intolerance for mistakes or a perceived need for help.[97] Intolerant cultures are less likely to embrace collaboration, as well as apply new or unproven knowledge in decision-making or problem solving.[98] Organizational intolerance stifles knowledge base growth and resultantly limits effective KM use as a strategic enabler.

Overcoming cultural barriers to knowledge creation, acquisition, and application requires a threefold strategic leader focus. First, leaders must provide an organizational vision that incorporates knowledge and learning.[99] Providing a vision is the "primary task of strategic leaders" and "sets the long-term direction for an organization."[100] In the context of KM, related tasks are to communicate, develop, and implement the vision in a way that promotes inter- and intra-organizational interaction and relationship building.[101] Second, leaders must develop and shape an organizational culture that values knowledge, collaboration, learning, and innovation. Organizational culture "supports and helps to communicate" the vision and is at the foundation of KM implementation and use.[102] Organizational cultures that value knowledge, collaboration, learning, and innovation create synergistic and mutually supportive environments where these characteristics thrive.[103] In shaping organizational cultures, KM tools such as social network analysis assist strategic leaders in understanding knowledge flows within and between organizations and provide a framework for identifying where gaps or barriers exist.[104] Once identified, leaders can focus resources and efforts in bridging knowledge gaps and overcoming identified barriers. Finally, strategic leaders must build and shape joint, interagency, and multi-national relationships that enable and encourage knowledge sharing, acquisition, and application.[105] These relationships are critical to realizing a whole of government KM approach and leveraging the collective capabilities of the multi-organizational network in achieving SSTRO unity of action and effort.

Recommendations

The preceding analysis explores KM as a strategic SSTRO enabler within an internal multi-organizational network environment and external VCUA environment. Knowledge obtained from conducting SSTRO and through addressing the myriad of associated wicked problems is a dynamic strategic resource requiring effective internal and cross-organizational management. As such, KM provides a critical "deliberate and systemic" enabling mechanism for coordinating and leveraging the "people, processes, technology, and organizational structure" for synergistic "knowledge creation, sharing, and application"

in successfully executing SSTRO.[106] The analysis contained herein also explores cultural barriers to KM implementation and use. Previous KM initiatives largely failed due to a primary focus on technology and knowledge codification while neglecting the socio-cultural aspects of KM that are integral to KM success. In this regard, it is critical for strategic leaders to focus on overcoming prohibitive cultural barriers as part of any KM endeavor. In the context of the overall analysis provided herein, three specific recommendations follow.

First, to meet the near-term challenges associated with SSTRO, the U.S. Department of Defense and the U.S. Department of State Office of the Coordinator for Reconstruction and Stabilization (S/CRS), under the authority granted in NSPD 44, must develop a formally recognized and KM-enabled SSTR community of practice.[107] The reasons for this are twofold. First, communities of practice facilitate the trust-building social construct necessary for increased tacit and explicit knowledge sharing and capture, accelerated learning, improved innovation, and more efficient and effective strategy implementation.[108] Second, communities of practice help mitigate negative knowledge attrition and enhance, through improved knowledge sharing within the network, the derived utility of other knowledge processes and KM best practices such as AARs and lessons learned.[109] A comprehensive social network analysis (SNA) should precede establishing the community to ensure effective capture and gap analysis of knowledge flows within the network. Further, strategic leaders within responsible SSTR organizations must champion the community and drive shared vision, norms, values, language, change, and investment to achieve synergistic accomplishment of objectives, goals, and overall SSTRO strategy.

Second, given the increasingly widespread recognition of KM as a strategic enabler, the collective National Security apparatus must develop and implement a whole of government KM strategy. The January 2009 U.S. Government *Counterinsurgency Guide* clearly articulates the primary justification for a whole of government KM strategy given "one of the most critical yet pervasive shortcomings that interagency operations face is the failure to manage and share knowledge."[110] A comprehensive strategy must encompass all facets of KM, specifically people, processes, technology, and organizational

structure, and must begin with strategic leadership. As expressed by organizational management author Peter Drucker:

> *One does not 'manage' people. The task is to lead people. And the goal is to make productive the specific strengths and knowledge of each individual.*[111]

Leadership is critical to KM strategy development and implementation as it drives the vision, cultural and structural change, process re-engineering, and technology investment essential to KM effort success.[112] Also critical are people as knowledge "exists within people, part and parcel of human complexity and unpredictability."[113] A whole of government KM strategy must first focus on socio-cultural aspects of KM, with process, technology, and structural aspects changed or designed to support.[114] Further, leveraging ongoing and planned KM efforts and lessons learned, including those derived from developing a SSTR community of practice, is essential to efficient and effective development of a more holistic strategy. Through holistic and effective implementation and use across and within the spectrum of U.S. agency functions, KM provides an integral and unifying tool for achieving national security objectives.

Finally, the U.S. Department of Defense, the U.S. Department of State, as well as the broader interagency must focus on becoming learning organizations. Learning organizations and "an organizational culture and structure that supports learning and the sharing and use of knowledge" are critical success factors in KM implementation and use.[115] Additionally, learning organizations emphasize shared vision, systems thinking, communities of practice, a learning culture, less hierarchical or more "self-organizing" structures, and an external environment focus.[116] These characteristics enable what Nonaka and Takeuchi metaphorically refer to as a "hypertext" organization, or one that leverages combinative and complementary bureaucracy and task force efficiencies and effectiveness.[117] Essentially, it is an organization with the "strategic ability to acquire, create, exploit, and accumulate new knowledge continuously and repeatedly in a cyclical process."[118] Thus, focusing on becoming learning organizations, in concert with KM implementation and use, will significantly improve U.S. federal agency agility, responsiveness, innovation, and decision-making in

addressing and managing the myriad of challenges in today's strategic environment.

Conclusion

The United States faces an increasingly complex and uncertain world typified by a host of wicked problems. The ongoing SSTRO efforts in post-conflict Iraq and Afghanistan are but one example of the challenges faced in this environment and one that clearly highlights the critical role that whole of government collaboration and knowledge sharing play in achieving strategic success. In responding to this environment, KM provides a powerful strategic enabler that facilitates improved collective agility, responsiveness, innovation, decision-making, and continuously expanding long-term problem solving capacity. Accordingly, U.S. federal agencies are increasingly focusing on KM to develop these strategic competencies – competencies that position the United States to more effectively meet U.S. national security objectives. Realizing KM as a strategic enabler, however, requires overcoming prohibitive cultural barriers. Foremost, this necessitates strategic leader focus as leadership drives the vision, culture, and relationships required for continuously improved knowledge sharing, acquisition, and application. Including and beyond SSTRO, overcoming barriers transcends organizational boundaries as responsibility for achieving unity of effort and overall strategic success falls on networks of knowledge and capabilities. As such, it is imperative that strategic leaders collectively pursue a whole of government KM strategy in concert with developing learning organizations. In today's environment, knowledge and continuous learning are vital strategic resources we can no longer afford to lose.

Endnotes

Preface

1. Reagan, Ronald. *National Security Decision Directive 130*. Washington, D.C.: The White House, 6 March 1984, http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm (accessed November 12, 2009).
2. Emergent NATO doctrine on Information Operations cites Diplomatic, Military and Economic activities as "Instruments of Power." It further states that Information, while not an instrument of power, forms a backdrop as all activity has an informational backdrop.
3. Neilson, Robert E. and Daniel T. Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," *National Security Strategy Quarterly* (Autumn 1999): 40.
4. R.S. Zaharna, "American Public Diplomacy in the Arab and Muslim World: A Strategic Communication Analysis," American University: Washington, DC, November 2001, http://www.fpif.org/pdf/reports/communication.pdf (accessed November 12, 2009).
5. Groh, Jeffrey L. and Dennis M. Murphy, "Landpower and Network Centric Operations: how information in today's battlespace can be exploited," NECWORKS, Issue 1, March 2006.

Section One: Information Effects in the Cognitive Dimension

Speed Versus Accuracy: A Zero Sum Game

1. Cori E. Dauber, "The Truth is out there: Responding to Insurgent Disinformation and Deception Operations," *Military Review* (January-February 2009): 13-14. Operation VALHALLA conducted on 26 March 2006 by 10th Special Forces Group and Iraqi Special Forces resulted in the discovery and destruction of an enemy weapons cache, the release of a badly beaten hostage being held by JAM members, the detention of 16 JAM, and 16-17 JAM killed. Only one Iraqi Soldier was injured during the operation.
2. "US Planes Hit Afghan Wedding Party, Killing 27," *The Sydney Morning News*, 07 July 2008, http://www.smh.com.au/cgi-bin/common/articles/2008/07/07 (accessed 23 April 2009). The event occurred 06 July 2008 in Nangarhar, Afghanistan. In the article a U.S. spokesman blamed the claims of civilian casualties on militant propaganda.
3. Candance Rondeauz, "Civilian Airstrike Deaths Probed," *The Washington Post*, 25 July 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/07/24/AR2008072403465 (accessed 23 April 2009).

4. Earl R. Carlson and Herbert I. Abelson, *Factors Affecting Credibility in Psychological Warfare Communications* (Human Resources Research Office, George Washington University, Silver Springs, MD, 1956): 7. Carlson and Abelson define credibility as a necessary condition for a communication to be effective and its contents to be believed by an audience. They stated credibility of a message exists with the audience.

5. Ibid., 12.

6. Ibid.,10-12.

7. Stephen M.R. Covey, *The Speed of Trust: The One Thing That Changes Everything* (Free Press, New York, NY, 2006): 54. Covey presents integrity, intent, capability, and results as the "4 cores of credibility." These are the elements that make or destroy credibility.

8. While Covey is generally categorized as a "self-help" author, the application of his criteria is appropriate here for several reasons. His schema was developed out of extensive experience in the business world, and has been applied successfully there. It is a reasonable assumption to make that the elements that define credibility for a business audience might work in other settings as well. Speculation is necessary where substantial empirical work on what establishes speaker credibility in cross-cultural settings is missing, but this does point to the need for such research going forward.

9. Ibid., Integrity, 59-72. Intent, 73-90. Capabilities, 91-108. Results, 109-125.

10. Carlson and Abelson, 24.

11. Timothy W. Coombs, *Crisis Management and Communication*, http://www.instituteforpr.org/essential_knowledge/detail/crisi_management_and_communications (accessed 30 April 2009).

12. Timothy W. Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, 2nd Ed. (Sage Publications, 2007): 130, http://www.sagepub.com/upm_data/14131.chapter8.pdf (accessed 30 April 2009).

13. Scott Russell, e-mail message to author, 13 January 2009. In 2007, MAJ Russell and I deployed to Afghanistan with the 13th PSYOP Battalion supporting CJTF-82. MAJ Russell, Tactical PSYOP Detachment 1320 Commander, served as the PSYOP officer for 4BCT, 82 ABN DIV. I served as the PSYOP Task Force-Afghanistan (POTF-AF) Commander responsible for planning and executing PSYOP for CJTF-82 and coordinating all U.S. PSYOP efforts in Afghanistan.

14. Coombs, *Crisis Management and Communication*.

15. Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, 129.

16. David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford, New York, 2009): 29. Kilcullen argues AQ statements

indicate a strategic intent to provoke the U.S. into actions that would destroy its credibility. The enemy understands credibility is based on action, not just words.

17. Scott Gerwehr and Kirk Hubbard, "What is Terrorism? Key Elements and History," *Psychology of Terrorism*, ed. Bruce Bongar, et al, (Oxford University Press, New York, 2007): 87. Gerwehr and Hubbard stated terrorism could be seen as a form of social influence, employing acts of extra-normal violence to influence a target population's emotions, motives, objective reasoning, perceptions, and ultimately behavior.

18. Kilcullen, *Accidental Guerrilla*, 300. Based on Gerwehr and Hubbard's description of terrorism as a form of social influence, the term "armed propaganda" aptly describes terrorism and acts of intimidation as used by insurgents and enemy forces in irregular warfare.

19. James N. Breckenridge and Philip G. Zimbardo, "The Strategy of Terrorism and Psychology of Maas-Mediated Fear," *Psychology of Terrorism*, ed. Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, Philip G. Zimbardo, (Oxford University Press, New York, 2007): 122. They stated this supports the asymmetrical principle. When applying this principle to irregular warfare, it is easier for insurgents to destroy public trust than it is for the government to build public trust.

20. Gerwehr and Hubbard, "What is Terrorism?," 91.

21. Ibid., 92-93.

22. Richard J. Josten, "Strategic Communications," *IO Sphere* (Joint Information Operations Center, Summer 2006) http://www.au.af.mil/inf-ops/iosphere/iosphere_summer06_josten.pdf (accessed 17 April 2009),19.

23. Anthony Pratkanis and Elliot Aronson, *Age of Propaganda: The Everyday Use and Abuse of Persuasion* (W.H. Freeman and Company, New York, 2001): 274.

24. Jason Motlagh, "Afghanistan's Propaganda War: The Taliban's Public Relations Machine," *USNEWS.COM*, posted 12 November 2008, http://www.usnews.com/article/news/iraq/2008/11/12/afghanistan-propaganda-war-the-taliban-public-relations-machine (accessed 15 April 2009).

25. Joanna Nathan, "Selling the Taliban," *The Wall Street Journal*, 02 September 2008, linked from *International Crisis Group* http://www.crisigroup.org/home/index.cfm?id=5656&1=1 (accessed 16 April 2009). The June 2008 jailbreak in Kandahar and the assault on the only five star hotel in Kabul; the February 2007 suicide bomber attack at Bagram Airbase while Vice President Cheney was visiting; and the 2007 South Korean hostage incident are a few of the examples of Taliban attacks that grabbed media headlines.

26. ABC News (Australian Broadcasting Corporation), "Taliban Show New Media Savvy," posted 20 August 2007, http://www.abc.net.au/news/stories/2007/08/20/2009153.htm (accessed 16 April 2009). From personal

experience, immediately following the 2007 suicide bomber attack at Bagram, inquiries by the media to the CJTF-82 PAO were made before news of the incident had been received in the CJTF HQs.

27. "Speed strategy" is a term developed by SGT Joe Atneosen during our 2007 rotation in Afghanistan. As a member of the POTF-AF S2 section, SGT Atneosen was responsible for tracking Taliban propaganda trends and methods, determining perceptions of the Afghan populace, and analysis that facilitated PSYOP planning and support for the CJTF-82 mission.

28. U.S. Department of the Army, *Counterinsurgency*, Field Manual 3-24, (Washington D.C.: U.S. Department of the Army, December 15, 2006): 1-103. If the insurgents maintain the momentum, they maintain the initiative.

29. Frans P.B. Osinga, *Science, Strategy, and War: The Strategic Theory of John Boyd* (Routledge, New York, 2007): 237.

30. Effective counter-propaganda seldom, if ever directly refutes each piece of enemy propaganda produced. An effective counter-propaganda program identifies and monitors enemy themes and incorporates discrediting/countering those themes with planned PSYOP programs and public information. It is part of the organization's day to day planned and executed actions and messages. An example would be Taliban night letters in Afghanistan. Night letters are normally hand written or crudely printed letters delivered at night to protect the source and add to the intimidation factor of just appearing at selected individual or public locations. The common theme of Taliban night letters is to not support the Government of Afghanistan and NATO forces or face punishment by the Taliban. Instead of refuting each night letter, counter the established theme. Directly refuting each night letter only highlights the piece of enemy propaganda and the fact the government of Afghanistan and NATO forces are unable to stop the dissemination of night letters. However, if you discredit the enemy's theme/message your render the night letters ineffective.

31. Osinga, *Science, Strategy, and War*, 231. This is the only diagram Boyd developed depicting the OODA loop. Diagrams of the rapid OODA loop as depicted in figure 1 were not developed by Boyd.

32. John Boyd, "The Strategic Game of ? and ?," ed. Chet Richards and Chuck Spinney (June 2006), http://www.d-n-i.net/boyd/strategic_game.ppt (accessed 19 April 2009): 33.

33. Ibid., 37.

34. Osinga, *Science, Strategy, and War*, 215.

35. Boyd, "The Strategic Game of ? and ?," 37.

36. Ibid., 36.

37. Osinga, *Science, Strategy, and War*, 230.

38. Ibid., 235-236.

39. Department of Defense, *Irregular Warfare (IW) Joint Operating Concept (JOC)*, Version 1.0, (Department of Defense, Washington D.C., 11 September 2007), http://www.dtic.mil/futurejointwarfare/concepts/iw_joc1_0.pdf (accessed 27 May 09), B-3. The term "indirect approach" has three distinct meanings within the context of IW: 1. Unbalance and dislocate adversaries by attacking them physically and psychologically where they are most vulnerable and unsuspecting, rather than where they are strongest or in the manner they expect to be attacked. 2. Empower, enable, and leverage IA and multinational strategic partners to attack adversaries militarily or non-militarily, rather than relying on direct and unilateral military confrontation by US joint forces. 3. Take actions with or against other states or armed groups in order to influence adversaries, rather than taking actions to influence adversaries directly.

40. U.S. Department of the Army, *Counterinsurgency*, 5-18.

41. Ibid., 5-18 – 5-34.

42. Chairman of the Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Department of Defense, Washington D.C. 13 February 2006): ix. JP3-13 defines IO as: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own." The specific effect IO is to achieve is to disrupt the adversarial decision making – enemy leaders and their networks. If IO is limited to integrating the core, specified and related capabilities to this target set as it was intended to do, it would be more effective and produce results.

43. Past experiences with several organizations have separated IO and other information activities into separate non-kinetic staff sections or organizations limiting access and integration into kinetic operational planning.

44. Strategic Communication, as defined in JP 1-02, is the "focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power." Strategic Communication is a coordination function to synchronize interagency and military information activities and action.

45. Heritage Lectures, No. 1065, "Public Diplomacy: Reinvigoration America's Strategic Communication Policy," presented by Edwin J. Feulner, Ph.D., Helle C. Dale, Colleen Graffy, Michael Doran, Ph.D., Joseph Duffy, Ph.D., Tony Blankley on February 13, 2008, (The Heritage Foundation, Washington D.C., March 14, 2008), http://www.heritage.org/research/nationalsecurity/upload/hl_1065.pdf (accessed 13 January 2009): 5. Colleen Graffy presented the concept of a pre-active approach as one that "anticipates and helps shape

stories" in the media. This concept was expanded by the author to include other aspects of social networking and actions required to shape the information environment including all key audiences.

Developing an Operational Strategic Communication Model for Counterinsurgency

1. U.S. Department of State, *QDR Execution Roadmap for Strategic Communications* (Washington, DC: U.S. Department of State, September 2006), 2.
2. Kenneth Payne, "Waging Communication War," *Parameters* 38, no. 2 (Summer 2008): 37.
3. Thomas X. Hammes, "Information Operations in 4GW," in *Global Insurgency and the Future of Armed Conflict*, ed. Terry Terriff, Aaron Karp and Regina Karp (New York, NY: Routledge, 2008): 204.
4. The author's personal experience in counterinsurgency has been in Afghanistan at the tactical level as a battalion commander in Operation Enduring Freedom (OEF) VI (July – November 2005), and at the operational level as the Director of Operations for Combined Joint Task Force (CJTF) 82 in OEF VIII (January 2007- April 2008).
5. U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, May 14, 2007): 1-9.
6. U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13 (Washington, DC: U.S. Joint Chiefs of Staff, February 13, 2006): GL-9.
7. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, April 12, 2001 as Amended Thru October 17, 2008): 442.
8. Ibid., 152.
9. Dennis M. Murphy, "The Trouble With Strategic Communication(s)," *IOSphere* (Winter 2008): 26.
10. U.S. Department of the Army, *Operations,* Field Manual 3-0 (Washington, DC: U.S. Department of the Army, February 27, 2008), A-1.
11. U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, I-9 – I-10.
12. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* 316.
13. U.S. Department of the Army, *Counterinsurgency,* Field Manual 3-24 (Washington, DC: U.S. Department of the Army, December 2006): 5-3.
14. Ibid.
15. Ibid., 5-5.

16. Ibid., 5-6.
17. Dennis M. Murphy, *Fighting Back: New Media and Military Operations* (Carlisle Barracks, PA: U.S. Army War College, Center for Strategic Leadership, 2008): 12.
18. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976): 89.
19. Barry E. Venable, "The Army and the Media," *Military Review* (January-February 2002): 71.
20. Clausewitz, *On War,* 77.
21. David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, CN: Praeger Security International, 1964): 9.
22. Colin S. Gray, "The American Way of War: Critique and Implications," in *Rethinking the Principles of War,* ed. Anthony D. McIvor (Annapolis, MD: Naval Institute Press, 2005): 27-33.
23. Ibid., 29.
24. Ibid.
25. Murphy, *Fighting Back: New Media and Military Operations*, 4.
26. Timothy L. Thomas, "Cyber Mobilization: A Growing Counterinsurgency Campaign," *IOSphere* (Summer 2006): 6.
27. Murphy, *Fighting Back: New Media and Military Operations*, 9.
28. Gray, "The American Way of War: Critique and Implications," 30.
29. James S. Corum, *Fighting the War On Terror: A Counterinsurgency Strategy* (St. Paul, MN: Zenith Press, 2007): 187.
30. Murphy, *Fighting Back: New Media and Military Operations*, 9.
31. Gray, "The American Way of War: Critique and Implications," 32.
32. John A. Nagl, *Learning to Eat Soup with a Knife* (Chicago, IL: University of Chicago Press, 2005): 205.
33. Galula, *Counterinsurgency Warfare: Theory and Practice*, 3.
34. Gray, "The American Way of War: Critique and Implications," 32.
35. Ibid., 33.
36. U.S. Department of Defense, *Strategic Communication Plan for Afghanistan* (Washington, DC: U.S. Department of Defense, September 2007): 1.
37. Combined Joint Task Force-82, "Command Brief," Bagram Airfield, Afghanistan, March 2008.
38. Deirdre Collings and Rafal Rohozinski, *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations, A Workshop Report* (Carlisle Barracks, PA, U.S. Army War College, 2006): 16.

39. U.S. Department of Defense, *Strategic Communication Plan for Afghanistan,* 2.
40. U.S. Joint Chiefs of Staff, *Joint Operations Planning,* Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, December 26, 2006): GL-18.
41. Ibid., GL-11.
42. Ibid., GL-17.

Empowering United States Public Diplomacy for the War of Ideas

1. George W. Bush, *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 2002): 9.
2. Ibid., 6.
3. Bruce Gregory, "Public Diplomacy and National Security: Lessons from the U.S. Experience," *Small Wars Journal* (April 2008), http://smallwarsjournal.com/mag/docs-temp/82-gregory.pdf (accessed January 21, 2009).
4. Kristin M. Lord, *Voices of America: U.S. Public Diplomacy for the 21st Century* (Washington, DC, The Foreign Policy Program at Brookings and The Brookings Project on U.S. Relations with the Islamic World, November 2008): 7.
5. David E. Morey, "Winning the War of Ideas," Testimony by the Co-Chairman of the Council on Foreign Relation's Independent Task Force on Public Diplomacy, delivered to the *Subcommittee on National Security, Emerging Threats and International Relations* (U.S. Congress, February 10, 2004): 2, http://www.au.af.mil/au/awc/awcgate/congress/public_diplomacy_morey_feb04.pdf (accessed December 12, 2008).
6. Donald Rumsfeld, "Rumsfeld: U.S. Losing War of Ideas," March 27, 2006, http://www.cbsnews.com/stories/2006/03/27/terror/main1442811.shtml (accessed January 6 2009).
7. George W. Bush, *U.S. National Strategy for Combating Terrorism* (Washington, DC, The White House, September 2006): 1, 23.
8. Sherifa D. Zuhur, *Precision in the Global War on Terror: Inciting Muslims through the War of Ideas* (Carlisle Barracks, PA, U.S. Army War College, Strategic Studies Institute, April 2008): 74, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB843.pdf (accessed December 10, 2008).
9. Adda B. Bozeman, "Iran: U.S. Foreign Policy and the Tradition of Persian Statecraft," *Orbis* 23, no. 2 (Summer 1979): 387-388.
10. Adam Garfinkle, "Comte's Caveat: How We Misunderstand Terrorism," *Orbis* 52, no. 3 (Summer 2008): 406-407.
11. G. John Ikenberry, "The Paradox of American Power: Why the World's Only Superpower Can't go it Alone, by Joseph S. Nye Jr, Oxford Univ. Press, 2002," [Book Review] *Foreign Affairs* 81, no. 2 (March/April 2002), http://www.

foreignaffairs.com/articles/57639/g-john-ikenberry/the-paradox-of-american-power-why-the-worlds-only-superpower-can (accessed December 10, 2008).

12. Kathy R. Fitzpatrick, *The Collapse of American Public Diplomacy* (Hamden, CT, Quinnipiac University, School of Communications, 2008): 4, http://www.publicdiplomacy.org/Fitzpatrick2008.pdf (accessed January 4, 2009).
13. Ambassador Pamela Hyde Smith, "Politics and Diplomacy: The Hard Road Back to Soft Power," *Georgetown Journal of International Affairs* 8 (Winter/Spring 2007): 4.
14. Rosaleen Smyth, "Mapping US Public Diplomacy in the 21st Century," *Australian Journal of International Affairs* 55, no. 3 (2001): 425.
15. Public Diplomacy Council, *A Call for Action on Public Diplomacy* (Washington, DC, Public Diplomacy Council, January 2005): 9.
16. U.S. Government Accountability Office, *U.S. Public Diplomacy: State Department Efforts to Engage Muslim Audiences Lack Certain Communication Elements and Face Significant Challenges*, GAO-06-535 (Washington DC, U.S. Government Accountability Office, May 2006): 18.
17. Ibid., 35-37.
18. Ibid., 35.
19. Bush, *The National Security Strategy of the United States of America*, 6.
20. Casimir A. Yost, "Assessing the Bush Administration's Foreign Policy," *National Interest* (May 14, 2003): 2.
21. Ibid.
22. Pew Global Attitudes Project, *America's Image Further Erodes, Europeans Want Weaker Ties* (Washington, DC: Pew Research Center, March 18 2003).
23. Ibid.
24. Brooks Kraft-Corbis, "The End of Cowboy Diplomacy," *Time* (July 17, 2006): 23.
25. Joseph S. Nye, Jr., "Public Diplomacy in the 21st Century," May 10, 2004, http://www.theglobalist.com/StoryId.aspx?StoryId=3885 (accessed August 8, 2008).
26. Joseph S. Nye, Jr., "The Decline of America's Soft Power, Why Washington Should Worry," *Foreign Affairs* 83, no. 3 (May-June 2004): 16-21.
27. Anne Gearan, "Hughes: Fixing US Image May Take Years," *Associated Press*, September 28, 2006, http://www.sfgate.com/cgi-bin/article.cgi?file=/n/a/2006/09/28/national/w132824D75.DTL&type=printable (accessed September 30, 2008).
28. Bozeman, "Iran: U.S. Foreign Policy and the Tradition of Persian Statecraft," 388.

29. Amir Taheri, "What Do Muslim's Think?" *American Interest* (May/June 2007): 6, http://www.the-american-interest.com.ezproxy.usawcpubs.org/ai2/article.cfm (accessed December 10, 2008).
30. Ibid.,13.
31. Ibid.,10.
32. Bozeman, "Iran: U.S. Foreign Policy and the Tradition of Persian Statecraft," 391.
33. Zeyno Baran, "Fighting the War of Ideas," *Foreign Affairs* 84, no. 6 (November/December 2005), http://www.foreignaffairs.com/articles/61200/zeyno-baran/fighting-the-war-of-ideas (accessed December 10, 2008).
34. Robert R. Reilly, "Winning the War of Ideas," September 22, 2007, linked from *The Public Diplomacy Home Page,* http://www.publicdiplomacy.org/85.htm (accessed December 10, 1008).
35. Ibid.
36. Ibid.
37. Garfinkle, "Comte's Caveat," 413.
38. Ibid., 406-408.
39. Ibid., 407-408.
40. Ibid., 408.
41. Ibid., 410.
42. Ibid.
43. Ibid.
44. Ibid.
45. Ibid., 412.
46. Ibid.
47. William Rosenau, "Waging the 'War of Ideas'," in *McGraw-Hill Homeland Security Handbook*, ed. David Kamien (New York, McGraw-Hill, 2006): 1132, http://www.rand.org/pubs/reprints/2006/RAND_RP1218.pdf (accessed January 6, 2009).
48. Gregory, "Public Diplomacy and National Security."
49. Antulio J. Echevarria II, *Wars of Ideas and The War of Ideas* (Carlisle Barracks, PA, U.S. Army War College, Strategic Studies Institute, June 2008): vii, http://www.StrategicStudiesInstitute.army.mil/pdffiles/PUB866.pdf (accessed December 29, 2008).
50. Robert Satloff, "How to Win The War Of Ideas," *The Washington Post*, November 10, 2007.
51. Ibid.

52. Echevarria, *Wars of Ideas and The War of Ideas*, 24.
53. Sun Tzu, *Art of War*, trans. Samuel B. Griffith (New York, Oxford University Press, 1971): 84.
54. John Hughes, "The Key to a Better U.S. Image," *The Christian Science Monitor* (June 26, 2008): 9, http://www.csmonitor.com/2008/0626/p09s03-coop.html (accessed February 2, 2009).
55. William J. Hybl, "Getting the People Part Right: A Report on the Human Resources Dimension of U.S. Public Diplomacy," The United States Advisory Commission on Public Diplomacy (Washington D.C., 2008): 5.
56. Smith, "Politics and Diplomacy: The Hard Road Back to Soft Power," 4.
57. Ibid.
58. Ibid.
59. Hybl, "Getting the People Part Right," 5.
60. Lord, *Voices of America*, 37.
61. Smith, "Politics and Diplomacy: The Hard Road Back to Soft Power," 4.
62. Hybl, "Getting the People Part Right," 4-5.
63. Ibid., 4.
64. Michele A. Flournoy and Tammy S. Schultz, *Shaping U.S. Ground Forces for the Future: Getting Expansion Right* (Washington, DC, Center for a New American Security, June 13, 2007): 10-11.
65. Anthony J. Blinken, "Winning the War of Ideas," *Washington Quarterly* 25, no. 2 (Spring 2002): 104.
66. Smith, "Politics and Diplomacy: The Hard Road Back to Soft Power," 3.
67. Ibid., 3-4.
68. U.S. Joint Forces Command, *The Joint Operating Environment 2008: Challenges and Implications for the Future Joint Force* (Washington, DC, U.S. Joint Forces Command, 2008): 26, https://us.jfcom.mil/sites/J5/j59/default.aspx (accessed April 2, 2009).
69. American Academy of Diplomacy, *A Foreign Affairs Budget for the Future: Fixing the Crisis in Diplomatic Readiness* (Washington, DC, American Academy of Diplomacy, October 2008): 3.
70. Carnes Lord and Helle C. Dale, "Public Diplomacy and the Cold War: Lessons Learned," *Heritage Foundation Backgrounder*, no. 2070 (September 18, 2007): 3, http://www.heritage.org/Research/NationalSecurity/bg2070.cfm (accessed February 2, 2009).
71. Ibid., 2.
72. Ibid., 7.

73. Stephen Johnson, Helle C. Dale, Patrick Cronin Ph.D., "Strengthening US Public Diplomacy Requires Organization, Coordination, and Strategy," *Heritage Foundation Backgrounder*, no. 1875 (August 5, 2005): 3, http://www.heritage.org/Research/PublicDiplomacy/bg1875.cmf (accessed February 2, 2009).
74. Fitzpatrick, *The Collapse of American Public Diplomacy*, 8.
75. Ibid.
76. Ibid.
77. Ibid., 8-9.
78. Reilly, "Winning the War of Ideas."
79. Fitzpatrick, *The Collapse of American Public Diplomacy*, 4.
80. American Academy of Diplomacy, *A Foreign Affairs Budget for the Future: Fixing the Crisis in Diplomatic Readiness*, 24.
81. Andrew Kohut, *Some Positive Signs for U.S. Image: Global Economic Gloom – China and India Notable Exceptions* (Washington, DC, Pew Research Center, Pew Global Attitudes Project, released June 12, 2008): 21.
82. Ibid.
83. Ibid.
84. Ibid.
85. Ibid.
86. Ibid.
87. Ibid., 24.
88. Ibid., 27.
89. Ibid., 28.
90. Ibid., 24.
91. Ibid.
92. "Iranian Public Opinion on Governance, Nuclear Weapons and Relations with the United States," linked from *WorldPublicOpinion.org*, 2008, http://www.worldpublicopinion.org/incl/printable_version.php?pnt=527 (accessed March 6, 2009).
93. Ibid.
94. "Iranians Favor Direct Talks with US on Shared Issues, Mutual Access for Journalists, More Trade," linked from *World Public Opinion.Org*, 2008, https://www.worldpublicopinion.org/incl/printable_version.pha?pnt=468 (accessed March 6, 2009).
95. Ibid.
96. Ibid.

97. "Iranian Public Opinion on Governance, Nuclear Weapons and Relations with the United States"
98. "Iranians Favor Direct Talks with US on Shared Issues, Mutual Access for Journalists, More Trade"
99. Ibid.
100. "Iranians Overwhelmingly Reject Bin Laden," linked from *World Public Opinion.Org*, 2006, https://www.worldpublicopinion.org/incl/printable_version.php? pnt=313 (accessed March 6, 2009). Similar data from 2008 addressing this same question is not available.
101. "Iranian Public Opinion on Governance, Nuclear Weapons and Relations with the United States"
102. "Iranians Oppose Producing Nuclear Weapons, Saying It Is Contrary to Islam", linked from *World Public Opinion.Org*, 2008, https://www.worldpublicopinion.org/incl/printable_version.php?pnt=469 (accessed March 6, 2009).
103. Ibid.
104. Ibid.
105. Ibid.
106. Ibid.
107. Ibid.
108. "Iranians and Americans Believe Islam and West Can Find Common Ground," linked from *World Public Opinion.Org*, January 30, 2007, https://www.worldpublicopinion.org/pipa/articles/brmiddleeastnafricara/312 (accessed March 6, 2009).
109. "Iranians Overwhelmingly Reject Bin Laden"
110. Ibid.
111. "Iranian Public Opinion on Governance, Nuclear Weapons and Relations with the United States"
112. Ibid.
113. "Iran Invests 2.5b in Stem Cell Research," linked from Payvand News (Iran), November 7, 2008, http://www.payvand.com/news/08/nov/1059.htlm (accessed March 10, 2009).
114. "Stem Cell Research in Iran," Science and Religion News, November 17, 2008, http://sciencereligionnews.blogspot.com/2008/09/stem-cell-research-in-iran.htlm (accessed March 10, 2009).
115. "Iranian Public Opinion on Governance, Nuclear Weapons and Relations with the United States"
116. Ibid.

117. U.S. Department of State, "Budget Summary and Summary Tables, FY 2008 Budget in Brief for U.S. Department of State," February 5, 2007, http://www.state.gov/s/d/rm/rls/bib/2008/html/79738.htm (accessed February 2, 2009).

118. Pew Research Center, *Some Positive Signs for U.S. Image: Global Economic Gloom – China and India Notable Exceptions*, 24-Nation Pew Attitudes Survey, The Pew Global Attitudes Project (June 2008): 28.

119. "Muslim Publics Oppose Al Qaeda's Terrorism, But Agree With its Goal of Driving US Forces Out," linked from *World Public Opinion.org*, 2008, http://www.worldpublicopinion.org/incl/printable_version.php?pnt=591 (accessed March 6, 2009).

120. Francis Fukuyama, "A New Era," *American Interest* (January-February 2009), http://www.the-american-interest.com/ai2/article.cfm?piece=535 (accessed March 3, 2009).

121. Ibid.

122. Ibid.

123. Steven Kull, Director, Program on International Policy Attitudes, *Iraqi Public Opinion on the Presence of US Troops*, Testimony before House Committee on Foreign Affairs, Subcommittee on International Organizations, Human Rights, and Oversight, linked from *World Public Opinion.org,* July 23, 2008, http://www.worldpublicopinion.org/incl/printable_version.php?pnt=517 (accessed March 6, 2009).

124. Ibid.

125. Ibid.

126. Ibid.

127. Ibid.

128. Lord and Dale, "Public Diplomacy and the Cold War"

129. Smith, "Politics and Diplomacy: The Hard Road Back to Soft Power," 6.

130. Lord and Dale, "Public Diplomacy and the Cold War"

National Communications Strategy

1. Rice, Condoleezza Rice. 2005 "Announcement of Nomination of Karen P. Hughes" 14 March 2005, http://www.state.gov/secretary/rm/2005/43385.htm

2. Helle C., Dale, "U.S. Public Diplomacy: The Search for a National Strategy," *Heritage Foundation*, Executive Memorandum, no. 1029, February 11, 2008

3. James Glassman, "Winning the War of Ideas," *The Washington Institute for Near East Policy*, July 8, 2008

4. Marc Lynch, Public diplomacy and strategic communication: "The Conversion," *Foreign Policy* (February 20, 2009), http://Lynch.foreignpolicy.

com/posts/2009/02/20/public_diplomacy_and_strategy_commincation (accessed March 30, 2009)

5. U.S. Congress, House, *Introduction of Strategic Communication Act of 2009*, 111th Cong., January 13, 2009

Section Two: Information Effects through Network and Knowledge-based Operations

Defining and Deterring Cyberwar

1. George W. Bush, *National Strategy to Secure Cyberspace* (Washington DC: The White House, February 2003): 5
2. Ibid.
3. Ibid.
4. Steven A. Hildreth, "Cyberwarfare," Congressional Research Service policy paper, June 19, 2001
5. Ibid.
6. Margaret Kane, "I Love You Email Worm Invades PCs," *ZDNet News*, May 4, 2000, http://news.zdnet.com/2100-9595_22-107318.html?legacy=zdnn, (accessed December 1, 2008).
7. Lincoln P. Bloomfield, Jr., "Cybersecurity: Ensuring the Safety and Security of Networked Information Systems," remarks at the Southeastern European Cybersecurity Conference, Sophia, Bulgaria, September 8, 2003, U.S. Department of State, http://www.state.gov/t/pm/rls/rm/23874.htm (accessed October 30, 2008).
8. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington DC, Dept. of Defense, April 12, 2001, amended through October 17, 2008): 459, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (accessed November 23, 2008).
9. Frontline: Cyberwar!, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings (accessed November 30, 2008).
10. Ibid.
11. Ibid., Bloomfield.
12. Christopher Rhoads, "Politics & Economics: Estonia Gauges Best Response to Cyber Attack," *The Wall Street Journal*, May 18, 2007.
13. "Cyberwar is genuine Threat," *RSA Conference Daily*, October 23, 2007, http://newsweaver.co.uk/rsaconference/e_article000935998.cfm?x=bbs1LTr,b8gpBBSr,w (accessed October 28, 2008).

14. "Cyberwarfare 101: Case Study of a Textbook Attack," *Stratfor* (April 18, 2008), http://www.stratfor.com/analysis/cyberwarfare_101_case_study_textbook_attack (accessed November 5, 2008).
15. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, Iss. 15.09 (August 21, 2007), http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia (accessed October 16, 2008)
16. Ibid., "Cyberwarfare 101: Case Study of a Textbook Attack"
17. Adam Smith, "Under Attack, Over the Net," *Time International* (June 11, 2007): 50.
18. Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," *Congressional Research Service Report for Congress*, RL32114 (January 29, 2008): 8.
19. John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 13, 2008.
20. Ibid.
21. Ibid.
22. "Russian Invasion of Georgia, Russian Cyberwar on Georgia," *Georgia Update*, http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf, (accessed November 14, 2008).
23. "Cyberwarfare 101: Georgia, Russia: The Cyberwarfare Angle" *Stratfor* (August 12, 2008), http://www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle, (accessed November 5, 2008).
24. Travis Wentworth, "Russian Nationalists Waged a Cyber War against Georgia. Fighting Back is Virtually Impossible," *Newsweek* (September 1, 2008).
25. Internet World Stats, http://www.internetworldstats.com/top20.htm (accessed November 11, 2008).
26. Bush, *National Strategy to Secure Cyberspace*, vii.
27. U.S. Army War College, "National Security Policy and Strategy Course Directive," (Carlisle Barracks, PA, 2008): App. I, 124.
28. Wilson, 22.
29. General Peter Pace, Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (Washington DC, Dept. of Defense, December 2006): C-1, http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed November 30, 2008).
30. World Federation of Scientists, "Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar," report and recommendations of the Permanent Monitoring Panel on Information Security (November 19, 2003): 10.
31. Ibid.

32. Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala*, Vol. 8, No. 1 (October 2008): 51.

33. Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Nework," *Security Focus* (August 19, 2003), http://www.securityfocus.com/news/6767 (accessed November 14, 2008).

34. Robert Lemos, "MSBlast and the Northeast Power Outage," *CNet News* (February 16, 2005), http://news.cnet.com/8301-10784_3-5579309-7.html (accessed December 1, 2008).

35. Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid" *CNN*, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html, (accessed October 28, 2008).

36. Ibid.

37. Brian Cashell, William D. Jackson, Mark Jicklin,et al., "The Economic Impact of Cyber Attacks," *CRS Report for Congress* RL 32331, April 1, 2004, CRS-1, http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf, (accessed December 1, 2008).

38. Cashell, et al., Summary page.

39. Ibid.

40. "US Warns of Possible Financial Cyber Attack" *NBC News and News Services* (November 30, 2006) http://www.msnbc.msn.com/id/15975889/ (accessed December 1, 2008).

41. Stratfor online, "Cyberwarfare 101: Case Study of a Textbook Attack," http://www.stratfor.com/analysis/cyberwarfare_101_case_study_textbook_attack, (accessed November 8, 2008).

42. Eneken Tikk, Kadri Kaska, Kristel Runnimeri, et al, "Georgian Cyber Attacks: Legal Lessons Identified," (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008): 7.

43. World Federation of Scientists, 9.

44. Fritz, 66.

45. Eneken Tikk, et al, 13.

46. Max Weber, *The Theory of Social and Economic Organization*, (New York: Collier-MacMillan, 1964): 154.

47. Richard W. Aldrich, "The International Legal Implications of Information Warfare," *Airpower Journal* (Fall 1996): 100, http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf, (accessed November 3, 2008).

48. Duncan B. Hollis, "E-war rules of engagement" *Los Angeles Times* (October 8, 2007): A15.

49. Dr. Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," http://www.maxwell.af.mil/au/awc/cyberspace/documents/Cyber%20Chapter%20Kuehl%20Final.doc (accessed November 3, 2008).
50. Ibid., 2.
51. Pace, 3.
52. Dr. Lani Kass, "A Warfighting Domain," AF Cyberspace Task Force briefing, (September 26, 2006): 14, http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf (accessed November 3, 2008).
53. JP 1-02, 141.
54. Joint Publication 3-13, "Information Operations," (Washington DC, February 13, 2006): I-1 – I-2.
55. Bush, 1.
56. Ibid.
57. JP 3-13, II-1.
58. Ibid., II-5.
59. Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly*, Issue 46 3d Quarter 2007 (Washington DC, National Defense University Press): 60, http://www.carlisle.army.mil/DIME/documents/Alexander.pdf, (accessed November, 23, 2008).
60. Walter G. Sharp, Jr., *Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research, 1999): 28.
61. United Nations Charter, Article 2(4), http://www.un.org/aboutun/charter/. (accessed November 4, 2008).
62. Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Falls Church, VA: Aegis Research, 2000): 37.
63. Ibid.
64. United Nations, Resolution 3314, "Definition of Aggression," December 14, 1974, http://www.un-documents.net/a29r3314.htm (accessed November 3, 2008).
65. Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Falls Church VA, Aegis Research, 2000): 81.
66. Bruno Simma, The Charter of the United Nations: A Commentary, (Oxford, UKI, Oxford University Press, 1994): 670.
67. United Nations, General Assembly Resolution 3314.
68. JP 1-02, 141.
69. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Colorado Springs,

CO: Institute for Information Technology, 1999): 17, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993&Location=U2&doc=GetTRDoc.pdf (accessed November 3, 2008).

70. Ibid., 17.

71. Sharp, 101.

72. Thomas Wingfield and James B. Michael, *An Introduction to Legal Aspects of Operations in Cyberspace* (Monterrey, CA, Naval Postgraduate School, April 28, 2004): 10.

73. Ibid.

74. Michael N. Schmitt, quoted in Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, 116.

75. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, 122.

76. Schmitt, 18-19.

77. Thomas Wingfield, James B. Michael, Duminda Wijesekera, *Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System* (Washington, DC, IEEE Computer Society, November 2003) http://www.au.af.mil/au/awc/awcgate/nps/ws09-with-pub-info.pdf (accessed November 10, 2008).

78. Ibid.

79. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*. 87-89.

80. Ibid, 90.

81. Ibid, 56.

82. Department of Defense, *Deterrence Operations Joint Operating Concept* (Washington DC, Department of Defense, December 2006): 5.

83. Colin S. Gray, "Deterrence and the Nature of Strategy," in *Deterrence in the 21st Century*, ed. Max G. Manwaring, (London, Frank Cass, 2001): 18.

84. Robert H. Dorff and Joseph R. Cerami, "Deterrence and Competitive Strategies: A New Look at an Old Concept," in *Deterrence in the 21st Century*, ed. Max G. Manwaring, (London, Frank Cass, 2001): 111.

85. Julian E. Barnes, "Hacking Could Become Weapon in US Arsenal," *Los Angeles Times*, September 28, 2008, http://www.latimes.com/news/nationworld/nation/la-na-cyber8-2008sep08,0,5570856,print.story (accessed November 4, 2008).

86. Pace, ix.

87. Ibid., 13.

88. General James Cartwright, quoted by David Blake, "Fighting in Cyberspace," *Military Periscope* (April 25, 2007), http://www.militaryperiscope.com/special/special-200704251756.shtml (accessed September 3, 2008).
89. Pace, 10.
90. "Military Ponders Cyber War Rules," *Los Angeles Times*, April 7, 2008.
91. Fritz, 42.
92. Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *The Washington Post* (February 7, 2003) http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38110-2003Feb6&notFound=true (accessed November 14, 2008).
93. General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," http://www.fas.org/irp/gao/aim96084.htm, (accessed November 4, 2008).
94. Bush, viii.
95. Fritz, 42.
96. United States Computer Emergency Response Team, http://www.us-cert.gov/aboutus.html (accessed November 12, 2008).
97. Ministry of Defence, Estonia, *Cyber Security Strategy* (Tallinn, Estonia, Ministry of Defence, 2008): 7.
98. Ibid., 4-5.
99. Charles W. Freeman, Jr., *Diplomatic Strategy and Tactics* (Washington D.C., U.S. Institute of Peace, 1997): 84.
100. Ibid.
101. Charles W. Freeman, Jr., Arts of Power: Statecraft and Diplomacy (Washington DC: US Institute of Peace, 1997): 38.
102. Ministry of Defence, Estonia, *Cyber Security Strategy*, 17.
103. Tikk, et al., 22.
104. Fritz, 61.
105. Tikk, et al., 22.
106. James B. Morell, *The Law of the Sea: The 1982 Treaty and Its Rejection by the United States* (London, UK, McFarland, 1992): 2.
107. Richard H. Wyman, "The First Rules of Air Warfare," *Air University Review*, March-April 1984 (Maxwell AFB, AL, Air University Press, 1984), http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/mar-apr/wyman.html (accessed December 1, 2008).

108. "A History of the Internet 1962-1992" *Computer History Museum*, http://www.computerhistory.org/internet_history/internet_history_90s.shtml (accessed December 1, 2008).
109. Fritz, 58.
110. Ministry of Defence, Estonia, *Cyber Security Strategy*, 21.
111. John T. Rourke and Mark A. Boyer, *International Politics on the World Stage*, glossary, http://highered.mcgraw-hill.com/sites/0073526304/student_view0/glossary.html (accessed on December 22, 2008).
112. World Federation of Scientists, 19.
113. Ministry of Defence, Estonia, *Cyber Security Strategy*, 17.
114. World Federation of Scientists, 22.
115. Ibid., 32.
116. George W. Bush, *The National Security Strategy of the United States of America* (Washington D.C., The White House, 2006): 36.
117. Kristin Archick, "Cybercrime: The Council of Europe Convention," *CRS Report for Congress* RS21208 (September 28, 2006): 1.
118. Ibid., 2-3.
119. Ministry of Defence, Estonia, *Cyber Security Strategy*, 18
120. Richard L. Kugler, *Policy Analysis in National Security Affairs: New Methods for a New Era* (Washington DC, National Defense University Press, 2006): 87.
121. Fritz, 43.
122. Declan McCullagh, "UN Agency Eyes Curbs on Internet Anonymity," *CNET News* (September 12, 2008), http://news.cnet.com/8301-13578_3-10040152-38.html?tag=nl.e703 (accessed October 16, 2008).
123. World Federation of Scientists, 27.
124. Ibid., 26.
125. Ibid., 18.

Impeding Network Centric Warfare: Combatant Command Information Technology Support

1. David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (The DoD Command and Control Research Program [CCRP] Publication Series, 1999): 35-36.
2. David S. Alberts and Richard E. Hayes, *Understanding Command and Control* (The DoD Command and Control Research Program [CCRP] Publication Series, 2006): 201.

3. Michael G. Mullen, *Capstone Concept for Joint Operations*, Version 3.0 (Washington, DC, U.S. Department of Defense, The Joint Staff, January 15, 2009): 4, 10, 33.
4. U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC, U.S. Department of Defense, The Joint Staff J7, May 14, 2007): III-12.
5. U.S. Department of Defense, *Functions of the Department of Defense and Its Major Components*, Directive 5100.01, (Washington, DC, U.S. Department of Defense, Assistant Secretary of Defense [Director of Administration and Management], August 1, 2002, certified current as of November 21, 2003): 3, 9-10.
6. Donald Rumsfeld, *Quadrennial Defense Review Report* (Washington, DC, The Department of Defense, February 6, 2006): 58-61.
7. Alberts and Hayes, *Understanding Command and Control*, 2.
8. Alberts, Garstka, and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 114.
9. Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, "Vision/Mission," http://www.defenselink.mil/cio-nii/docs/card.pdf (accessed January 11, 2009).
10. DISA Direct Home Page, "Defense Working Capital Fund (DWCF) Telecommunications Services Billing Prices for FY 2009," https://www.disadirect.disa.mil/products/asp/BillingRates/Final_DWCF_FY09_Price_Book_Ver11.pdf (accessed January 11, 2009), 3-31.
11. U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, Joint Publication 1, III-14.
12. U.S. Strategic Command, "U.S. Strategic Command Snapshot," http://www.stratcom.mil/fact_sheets/SnapShot.doc (accessed January 14, 2009).
13. U.S. Strategic Command, "U.S. Strategic Command Snapshot," http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html (accessed January 15, 2009).
14. U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, Joint Publication 1, III-2 – III-3.
15. For example, EUCOM Directive 50-1 defines the relationship between U.S. Army Europe – as the supporting "executive agent" – and EUCOM. ED 50-1 predates desktop computing, but does address communications support in the form of telephones and messaging.
16. Two of the most pertinent directives are *Management of DoD Information Resources and Information Technology*, Directive 8000.01 and *Information Technology Portfolio Management*, Directive 8115.01.
17. U.S. Department of Defense, *Management of DoD Information Resources and Information Technology*, Directive 8000.01 (Washington, DC, U.S. Department

of Defense, Assistant Secretary of Defense, Networks and Information Integration, February 27, 2002, certified current as of April 23, 2007): 3.

18. U.S. Department of Defense, *Information Technology Portfolio Management*, Directive 8115.01, (Washington, DC, U.S. Department of Defense, Assistant Secretary of Defense, Networks and Information Integration), October 10, 2005): 2-3.

19. U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Directive 8320.02 (Washington, DC, U.S. Department of Defense, Assistant Secretary of Defense, Networks and Information Integration/ Department of Defense Chief Information Officer, December 2, 2004, certified current as of April 23, 2007): 2-3.

20. U.S. Department of Defense, *Guidance for Implementing Net-Centric Data Sharing*, Guidance 8320.02-G (Washington, DC, U.S. Department of Defense, Assistant Secretary of Defense, Networks and Information Integration/ Department of Defense Chief Information Officer, April 12, 2006): 11-15.

21. U.S. Department of Defense, *Unique Identification (UID) Standards for a Net-Centric Department of Defense*, Directive 8320.03 (Washington, DC, U.S. Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics/Under Secretary of Defense for Personnel and Readiness, March 23, 2007): 5.

22. The Joint Chiefs of Staff, Joint Communications Systems, Joint Pub 6-0 (Washington, DC: U.S. Department of Defense, The Joint Staff J6, March 20, 2006): III-4.

23. Program Executive Office - Enterprise Information Systems, "Navy Marine Corps Intranet (NMCI)," https://enterprise.spawar.navy.mil/cmt_uploads/28/ NMCI%20BLII-ONEnet.pdf (accessed January 12, 2009).

24. U.S. Government Accountability Office, *Information Technology: DOD Needs to Ensure That Navy Marine Corps Intranet Program Is Meeting Goals and Satisfying Customers* (Washington, DCm U.S. Government Accountability Office, December 2006): 2-5.

25. Cynthia Rettig, "The Trouble with Enterprise Software," *MIT Sloan Management Review* 49, no. 1 (Fall 2007): 21-22.

26. U.S. General Services Administration Millennia web page, http://www.gsa.gov/millennia (accessed January 12, 2009).

27. With the exception of information the users placed in group-accessible network storage; this is not normally part of the tasker management business process and the data is not meta-tagged. A discussion of the structure and management of group-accessible network storage is an important part of information sharing and thus NCW, but beyond the scope of this paper.

28. U.S. Department of Defense, "Defense Information Systems Agency Global Command and Control System – Joint," http://www.disa.mil/gccs-j/ (accessed January 12, 2009).

29. John E. Ettlie et al., "Strategic predictors of successful enterprise system deployment," *International Journal of Operations & Production Management* 25, no. 10 (2005): 956.

30. U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Directive 8320.2 (December 2004): 2-3.

31. Sharon A. Houy, "Working Together: Why DIA Now Employs Combatant Command Intel Agents," *Armed Forces Journal*, (December 2008): 34-37.

Knowledge Centric Warfare: An Introduction

1. Adm Mike. G. Mullen, *Capstone Concept for Joint Operations* (Washington, DC: U.S. Joint Chiefs of Staff, January 15, 2009): iii.

2. Ibid., iv.

3. Ibid.

4. Paul W. Phister Jr. and Igor G. Plonish, *Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare.* (Rome, NY: Air Force Research Laboratory, June, 2004): 8.

5. Ibid.

6. Gen Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred A. Knopf, 2007): 19.

7. Dr. Michael Evans, "Knowledge Management and Warfare in the Information Age" briefing slides (Canberra, AU, Land Warfare Studies Centre, 2002)

8. Ibid.

9. Adapted from U.S. Army War College, Information Operations Primer: *Fundamentals of Information Operations* (Carlisle Barracks, PA: U.S. Army War College, Department of Military Strategy, Planning, and Operations and Center for Strategic Leadership, November, 2008): 2.

10. David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: DoD Command and Control Research Program, 2003): 113.

11. Alberts and Hayes, 15.

12. Matthias Steup, "Epistemology," in *The Stanford Encyclopedia of Philosophy* (Winter 2008 Edition), http://plato.stanford.edu/archives/win2008/entries/epistemology/ (accessed March 17, 2009).

13. Svavar Hrafn Svavarsson, "Pyrrho's Dogmatic Nature," *Classical Quarterly* 52, no. 1 (January 1, 2002): 248-256, in ProQuest (accessed March 23, 2009).

14. Peter Markie, "Rationalism vs. Empiricism," in *The Stanford Encyclopedia of Philosophy* (Fall 2008 Edition), http://plato.stanford.edu/archives/fall2008/ entries/ rationalism-empiricism/ (accessed March 15, 2009).
15. Peter D. Klein, "Epistemology," in *Routledge Encyclopedia of Philosophy* (London: Routledge 1998, 2005), http://www.rep.routledge.com/article/ P059 (accessed March 24, 2009).
16. Markie, "Rationalism vs. Empiricism."
17. Steup, "Epistemology."
18. Ibid.
19. Ibid.
20. Although the truth-condition enjoys nearly universal consent, there is a reasonable objection to it. Consider Newtonian Physics as a part of our overall scientific knowledge. But Newtonian Physics is false. Is it possible to know something that is false? The answer is no, with a two-fold caveat. The first is that when we clam to "know" Newtonian Physics, we are claiming to understand the explanatory power of the theory in the realm in which it applies, implying an understanding of recently discovered weaknesses - a true assertion. Secondly, we can distinguish between Newtonian physics and updated theoretical physics at the cutting edge where the more recent absorbs the former and explains how and where Newtonian Physics fails.
21. A famous article by Edmund Gettier in 1963 challenges JTB. The "Gettier Problem" involves the transference of justification from an ultimately false belief to a belief that is coincidentally true. Both propositions have met ascension criterion for knowledge, yet one of the propositions is false and thus not knowledge.
22. "Cognition," *Encyclopedia Britannica,* online 2009, http://www.britannica. com/EBchecked/ topic/124474/cognition (accessed February 01, 2009).
23. Paul Thagard, Mind: Introduction to Cognitive Science, 2nd ed., (Cambridge, MA: MIT Press, 2005): 10.
24. Martin Ryder, "Semiotics: Language and Culture" (May, 2004), http://carbon. cudenver. edu/~mryder/semiotics_este.html (accessed March 21, 2009).
25. Peter Brödner, "The Misery of Digital Organisations and the Semiotic Nature of IT," *AI & Society* 23, no. 3 (May 1, 2009): 331-351, in ProQuest (accessed March 23, 2009).
26. Brendan S. Gillon, "On the Semantics/Pragmatics Distinction." *Synthese* 165, no. 3 (December 1, 2008): 373-384, in ProQuest (accessed March 23, 2009).
27. Ikujiro Nonaka, "A Dynamic Theory of Organizational Knowledge Creation." *Organization Science* 5, no. 1 (1994): 19, in EBSCO (accessed March 19, 2009).

28. F. Dretske, *Knowledge and the Flow of Information* (Cambridge, MA: MIT Press. 1981): 44, 86.
29. Nonaka, "A Dynamic Theory of Organizational Knowledge Creation," 14.
30. Ibid., 19.
31. Ibid.,18.
32. Torsten Ringberg and Markus Reihlen. "Socio-Cognitive Approach to Knowledge Transfer," *Journal of Management Studies*, 45, no. 5 (July 2008).
33. Robert L. Cambell, "Jean Piaget's Genetic Epistemology: Appreciation and Critique," Revised version of two lectures presented at the Institute of Objectivist Studies Summer Seminar, Charlottesville, VA, July 7 and 8, 2006, http://hubcap.clemson.edu/~campber/piaget.html (accessed March 23, 2009).
34. R. Vanden, *Technology Based Learning Environment Designs for Ill-Structured Knowledge Domains*, Unpublished Thesis (Ontario: University of Guelph, 1998).
35. A. Lauzon, "Situating Cognition and Crossing Borders: Resisting the homogeny of Mediated Education." *British Journal of Educational Technology*, 30, no. 3 (1999) in EBSCO (accessed March 4, 2009).
36. Ibid.
37. CoP research adapted from a paper written by the author to satisfy course requirements at Walden University, March, 2007.
38. An excellent description on the application of a CoP in the U.S. Army is *Company Command: Unleashing the Power of the Army Profession* (West Point, NY: Center for Leader Development and Organizational Learning, 2005).
39. J. Lave and E. Wenger, *Situated Learning* (Cambridge, MA: Cambridge University Press, 1991).
40. E. Wenger, R. McDermott, and W. Snyder, *Cultivating Communities of Practice: A Guide to Managing Knowledge* (Boston: Harvard Business School Press, 2002).
41. Ibid.
42. C. Elmholdt, "Knowledge Management and the Practice of Knowledge Sharing and Learning at Work: A Case Study." *Studies in Continuing Education* 26, no. 2 (2004).
43. Ikujiro Nonaka, "The Knowledge Creating Company." *Harvard Business Review* 85, no. 7/8: (1991): 162-171.
44. E Wenger. Communities of Practice: Learning, Meaning and Identity (New York: Cambridge University Press, 1998).
45. Nonaka, "The Knowledge Creating Company."

46. K. Dalkir, *Knowledge Management in Theory and Practice* (New York: Elsevier Butterworth Heinemann, 2005).
47. Wenger, *Cultivating Communities of Practice: A Guide to Managing Knowledge*, 45-47
48. Ibid.
49. Dalkir, *Knowledge Management in Theory and Practice*.
50. A. Kim, *Community Building on the Web*. (Berkeley, CA: Peachpit Press, 2000).
51. L. Fisher, "Sustaining Communities of Practice in the Workplace: A Case Study," *STC Proceedings* (2004), in EBSCO (accessed February 15, 2008).
52. Ibid.
53. Kim, *Community Building on the Web*.
54. Fisher, "Sustaining Communities of Practice in the Workplace: A Case Study," 37.
55. G. Lakomski, "On Knowing in Context," *British Journal of Management* 15 (2004): 89-95.
56. Learning Theories Knowledgebase, "Learning Theories & Models," http://www.learning-theories.com/problem-based-learning-pbl.html (accessed March 24th, 2009).
57. A. Hemre, "Building and Sustaining Communities of Practice at Ericsson Research Canada," in *Knowledge Management Tools and Techniques*, ed. M. Rao (Burlington, MA: Butterworth-Heinemann, 2005).
58. Wenger, *Cultivating Communities of Practice: A Guide to Managing Knowledge*, 141.
59. Ringberg and Reihlen, "Socio-Cognitive Approach to Knowledge Transfer," 921.
60. Ibid., 919.
61. Ibid., 924.
62. Ibid.
63. Figure from Ringberg and Reihlen, "Socio-Cognitive Approach to Knowledge Transfer," 923, modified to reflect divergent and convergent creative processes associated with socialization as taught in the U.S. Army War College's Strategic Thinking syllabus.
64. Ibid., 925.
65. Ibid., 926.
66. Ibid., 928.
67. Ibid., 926.

68. Brian Robinson, "Army retools knowledge culture," *Federal Computer Week*, (September 05, 2008) http://fcw.com/Articles/2008/09/05/Army-retools-knowledge-culture.aspx (accessed March 23, 2009).

69. David S. Alberts, John J. Garstka and Fredrick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, DC: DoD C4ISR Cooperative Research Program, 1999): 29.

70. Susan Smith Nash "Network Centric Warfare and Implications for Distributed Education," *Online Learning*, April 9, 2005, http://www.xplanazine.com/2005/04/network-centric-warfare-and-implications-for-distributed-education (accessed March 15, 2009).

71. CDR Philip G. Pattee, USN (Ret), in "Network Centric Operations: A Need for Adaptation and Efficiency," *Air & Space Power Journal*, (Spring 2008), makes the specific point that while viewing the strategic environment as a Complex Adaptive System, social networks must include diversity beyond the DoD in what he calls "networked national security."

72. Tom Czerwinski, *Coping with the Bounds: Speculations on Nonlinearity in Military Affairs* (Washington, DC: DoD Command and Control Research Program,1998): 158.

73. Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 65.

74. Adapted from U.S. Department of the Army, *Knowledge Management*, Field Manual 6-01 (Washington DC: U.S. Department of the Army, August 29, 2008), and Alberts, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 29.

75. Robinson, "Army retools knowledge culture."

76. U.S. Department of the Army, *Knowledge Management*, Field Manual 6-01.1 (Washington DC: U.S. Department of the Army, August 29, 2008).

77. Phister and Plonish, *Information and Knowledge Centric Warfare: the Next Steps in the Evolution of Warfare*.

78. Peter Schwartz, *Inevitable Surprises* (New York: Gotham Books, 2003), 233.

Enabling Security, Stability, Transition, and Reconstruction Operations through Knowledge Management

1. Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in General Theory of Planning," *Policy Sciences* 4 (1973): 155-169. See also: Jeff Conklin, "Wicked Problems and Social Complexity," in *Dialogue Mapping: Building Shared Understanding of Wicked Problems* (Chichester, England: John Wiley & Sons, 2006): 3-23. A discussion of ill-structured problems may be found in U.S. Department of the Army, *Commander's Appreciation and Campaign Design*,

Training and Doctrine Command Pamphlet 525-5-500 (Fort Monroe, VA: U.S. Department of the Army, January 28, 2008), 9-11.

2. COL Stephen A. Shambach, ed., "The Strategic Leadership Environment," *Strategic Leadership Primer*, 2nd ed. (Carlisle Barracks, PA: U.S. Army War College, Department of Command, Leadership and Management, 2004): 12-13.

3. For the purposes of this paper, SSTR encompasses those activities, missions, and efforts as outlined or defined in the following sources and references embedded in these sources:

   - George W. Bush, *National Security Presidential Directive/NSPD-44* (Washington, D.C.: The White House, 7 December 2005): 1-6.
   - U.S. Department of Defense, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations*, Directive 3000.05 (Washington, D.C.: U.S. Department of Defense, November 28, 2005): 1-11.
   - COL David B. Haight, *Preparing Military Leaders for Security, Stability, Transition and Reconstruction Operations*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, March 30, 2007): 2.

4. Bush, *National Security Presidential Directive/NSPD-44*, 2.

5. Rahinah Ibrahim and Mark Nissen, "Discontinuity in Organizations: Developing a Knowledge-Based Organizational Performance Model for Discontinuous Membership," *International Journal of Knowledge Management* 3, no. 1 (January-March 2007): 10-28.

6. Edward P. Weber and Anne M. Khademian, "Wicked Problems, Knowledge Challenges, and Collaborative Capacity Builders in Network Settings," *Public Administration Review* 68, no. 2 (March-April 2008): 336.

7. Ibid., 334-339.

8. U.S. Department of the Army, *Commander's Appreciation and Campaign Design*, 13-14.

9. Beatriz Munoz-Seca and Josep Riverola, *Problem-Driven Management: Achieving Improvement in Operations through Knowledge Management* (New York, NY: Palgrave Macmillan, 2004): 6.

10. Jozef Loermans, "Synergizing the Learning Organization and Knowledge Management," *Journal of Knowledge Management* 6, no. 3 (2002): 285-294.

11. Lena Aggestam, "Learning Organization or Knowledge Management – Which Came First, The Chicken or the Egg?" *Information Technology and Control* 35, no. 3A (2006): 299.

12. David A. Garvin, "Building a Learning Organization," *Harvard Business Review on Knowledge Management* (Boston, MA: Harvard Business School Publishing, 1998), 51.

13. Aggestam, "Learning Organization or Knowledge Management – Which Came First, The Chicken or the Egg?," 298-300.
14. Peter Senge, *The Fifth Discipline: The Art & Practice of The Learning Organization* (New York, NY: Currency Doubleday, 1990): 6-11.
15. Ibid., 69.
16. Chris Argyris, *Reasons and Rationalizations: The Limits to Organizational Knowledge* (New York, NY: Oxford University Press, 2004): 10.
17. Thomas H. Davenport and Laurence Prusak, *Working Knowledge* (Boston, MA: Harvard Business School Press, 1998): 5.
18. Ibid., 2.
19. Ibid., 4.
20. Ikujiro Nonaka and Hirotaka Takeuchi, *The Knowledge-Creating Company* (New York, NY: Oxford University Press, 1995): 58.
21. Davenport and Prusak, *Working Knowledge*, 6.
22. Ibid., 12.
23. Nonaka and Takeuchi, *The Knowledge-Creating Company*, 8-9. See also: Verna Allee, *The Future of Knowledge: Increasing Prosperity through Value Networks* (Burlington, MA: Elsevier Science, 2003): 97.
24. Ibid. Also, Kimiz Dalkir, *Knowledge Management in Theory and Practice* (Burlington, MA: Elsevier Butterworth-Heinemann, 2005): 8.
25. Nonaka and Takeuchi, *The Knowledge-Creating Company*, 62-73. The Nonaka and Takeuchi model is referred to as the SECI model of organizational knowledge creation.
26. American Productivity & Quality Center (APQC), *Retaining Valuable Knowledge: Proactive Strategies to Deal With a Shifting Work Force* (Texas: American Productivity & Quality Center, 2002), 7. A functional definition of Knowledge Management is "a systematic process of connecting people to people and people to the knowledge and information they need to effectively perform and create new knowledge. The goal of a knowledge management initiative is to enhance the performance of the organization and the people in it, through the identification, capture, validation, and transfer of knowledge."
27. Dalkir, *Knowledge Management in Theory and Practice*, 43.
28. Peter F. Drucker, *Post-Capitalist Society* (New York, NY: HarperCollins, 1993): 6-8.
29. Michael E. D. Koenig and T. Kanti Srikantaiah, eds., *Knowledge Management Lessons Learned: What Works and What Doesn't* (Medford, NJ: Information Today, Inc., 2004): 127.
30. Amrit Tiwana, *The Knowledge Management Toolkit: Orchestrating IT, Strategy, and Knowledge Platforms* (Upper Saddle River, NJ: Prentice Hall, 2002): 6.

31. Davenport and Prusak, *Working Knowledge*, 15-17.

32. Annick Willem and Marc Buelens, "Knowledge Sharing in Public Sector Organizations: The Effect of Organizational Characteristics on Interdepartmental Knowledge Sharing," *Journal of Public Administration Research and Theory* 17 (January 2007): 581.

33. Elsa Rhoads, Kevin J. O'Sullivan, and Michael Stankowsky, "An Evaluation of Factors that Influence the Success of Knowledge Management Practices in U.S. Federal Agencies," *International Journal of Knowledge Management* 3, no. 2 (April-June 2007): 32.

34. Davenport and Prusak, *Working Knowledge*, 8. See also American Productivity & Quality Center (APQC), *Retaining Valuable Knowledge: Proactive Strategies to Deal With a Shifting Work Force*, 46. Additional information on CALL, the Battle Command Knowledge System, and other U.S. Army KM information can be accessed through the U.S. Army Combined Arms Center website at http://usacac.army.mil/cac2/index.asp.

35. U.S. Army Chief of Staff, General George W. Casey, Jr. and U.S. Secretary of the Army Pete Geren, "Army Knowledge Management Principles," memorandum for distribution to U.S. Department of the Army commands, July 23, 2008. See also: U.S. Department of the Army, *Operations*, Field Manual 3-0 (Washington, D.C.: U.S. Department of the Army, February 27, 2008): 7-10. The U.S. Army is incorporating KM into capstone Field Manuals. As an example, FM 3-0, *Operations*, specifically identifies KM as "the art of creating, organizing, applying, and transferring knowledge to facilitate situational understanding and decisionmaking. Knowledge management supports improving organizational learning, innovation, and performance. Knowledge management processes ensure that knowledge products and services are relevant, accurate, timely, and useable to commanders and decisionmakers." The "Knowledge and Information Management" section also identifies the KM components of people, processes, and technology.

36. R. William Maule, "Military Knowledge Management," *Encyclopedia of Knowledge Management*, ed. David G. Schwartz (Hershey, PA: Idea Group Reference, 2006): 628-630.

37. Ibid., 628. See also: Farida Hasanali et al., *Communities of Practice: A Guide for Your Journey to Knowledge Management Best Practices* (Houston, TX: American Productivity & Quality Center, 2002): 1-7. APQC defines communities as: "Networks of people – small and large – who come together to share ideas with and learn from one another in physical and virtual space. These communities of practice, of interest, and of learning are held together by a common purpose or mission. They are sustained by a desire to share experiences, insights, and best practices."

38. Summer E. Bartczak, Jason M. Turner, and Ellen C. England, "Challenges in Developing a Knowledge Management Strategy: A Case Study of the Air Force

Material Command," *International Journal of Knowledge Management* 4, no. 1 (January-March 2008): 49.

39. Maule, "Military Knowledge Management," 628.

40. Rhoads, O'Sullivan and Stankowsky, "An Evaluation of Factors that Influence the Success of Knowledge Management Practices in U.S. Federal Agencies," 32. See also: Thomas H. Kean and Lee H. Hamilton, *The 9/11 Commission Report* (Washington, D.C.: National Commission on Terrorist Attacks Upon the United States, 2004): 416-419, http://www.9-11commission.gov/report/911Report.pdf (accessed February 28, 2009). Section 13.3 (page 417) specified promoting a "need to share culture of integration" and included the recommendation "information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge."

41. Ibid.

42. Terrence K. Kelly and Thomas S. Szayhna, *Stabilization and Reconstruction Staffing: Developing U.S. Civilian Personnel Capabilities* (Santa Monica, CA: RAND Corporation, 2008): 68.

43. Project on National Security Reform, Forging a New Shield (Washington, DC: Project on National Security Reform, November 2008): A8-697.

44. Rittel and Webber, "Dilemmas in General Theory of Planning," 160-162.

45. U.S. Department of the Army, *Stability Operations*, Field Manual 3-07 (Washington, D.C.: U.S. Department of the Army, October 6, 2008): 4-5. U.S. Army doctrine on knowledge management is found in U.S. Department of the Army, Knowledge Management Section, Field Manual 6-01.1 (Washington, D.C.: U.S. Department of the Army, August 29, 2008). See also: U.S. Department of the Army, *Operations*, Field Manual 3-0 (Washington, D.C.: U.S. Department of the Army, February 27, 2008): 7-10.

46. LTC Howard Lim, "Knowledge Management at MNC-I: Trends, Challenges, and Opportunties," October 2008, brief linked from the United States Army Combined Arms Center Home Page, Center for Army Lessons Learned at http://usacac.army.mil/cac2/call/index.asp.

47. Rhoads, O'Sullivan and Stankowsky, "An Evaluation of Factors that Influence the Success of Knowledge Management Practices in U.S. Federal Agencies," 35.

48. U.S. Joint Chiefs of Staff, Capstone Concept for Joint Operations Version 3.0 (Washington, D.C.: U.S. Joint Chiefs of Staff, January 15, 2009): 6.

49. 49 Donald Hislop, *Knowledge Management in Organizations: A Critical Introduction* (New York, NY: Oxford University Press, 2005): 44-54.

50. Chyan Yang and Hsueh-Chuan Yen, "A Viable Systems Perspective to Knowledge Management," *Kybernetes* 36, no. 5/6 (2007): 644-648.

51. S. Vassiliadis, M. Kohne, and J. Barber, "Are Networks the Obvious Choice? When to Choose the Network Option," in *Getting Real about Knowledge Networks* (New York, NY: Palgrave Macmillan, 2006): 109-110.

52. Ibid., 183-207.

53. The Combined Security Transition Command – Afghanistan Home Page, http://www.cstc-a.com (accessed 14 November 2008).

54. North Atlantic Treaty Organization (NATO) International Security Assistance Force (ISAF) Home Page, http://www.nato.int/isaf/ (accessed December 10, 2008). Effective October 5, 2006, ISAF assumed overall responsibility for Afghanistan security and stability efforts.

55. Dalkir, *Knowledge Management in Theory and Practice*, 69. The definition of complex adaptive systems is "organizations that are composed of a large number of self-organizing components, each of which seeks to maximize its own specific goals but which also operates according to the rules and context of relationships with the other components and the external world." Component members of the CSTC-A staff are empowered to self-organize but are hierarchically part of the CSTC-A organization. As such the complex adaptive system represented by CSTC-A is considered intelligent.

56. Ibid., 70.

57. Ibid., 69-70.

58. Ibid., 70-71.

59. Ibid.

60. Ibid.

61. Ibid., 71.

62. Hislop, *Knowledge Management in Organizations: A Critical Introduction*, 44.

63. Gillian Wright and Andrew Taylor, "Strategic Knowledge Sharing for Improved Public Service Delivery: Managing an Innovative Culture for Effective Partnerships," in *Knowledge Management: Current Issues and Challenges*, ed. Elayne Coakes (Hershey, PA: IRM Press, 2003): 190.

64. Kenneth A. Grant and Candace T. Grant, "Developing a Model of Next Generation Knowledge Management," *Issues in Informing Science and Information Technology*, no. 5 (2008): 580.

65. Ibid., 580-587.

66. Grant and Grant, "Developing a Model of Next Generation Knowledge Management," 580-587.

67. Dalkir, *Knowledge Management in Theory and Practice*, 179. Dalkir as well as Nonaka and Takeuchi use E. Schein's (1985 and 1999) definition of organizational culture as "a pattern of basic assumptions—invented, discovered, or developed by a given group as it learns to cope with its problems of external

adaptation and internal integration—that has worked well enough to be considered valid and therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems."

68. Hislop, *Knowledge Management in Organizations: A Critical Introduction*, 46.
69. Yang and Yen, "A Viable Systems Perspective to Knowledge Management," 647.
70. Nonaka and Takeuchi, *The Knowledge-Creating Company*, 85.
71. Dalkir, *Knowledge Management in Theory and Practic*e, 185.
72. Hislop, *Knowledge Management in Organizations: A Critical Introduction*, 51.
73. Jennifer Lewis Priestley and Subhashish Samaddar, "Multi-Organizational Networks: Three Antecedents of Knowledge Transfer," *International Journal of Knowledge Management* 3, no. 1 (January-March 2007): 87. Absorptive capacity is defined as "an organization's ability to recognize the value of external information, assimilate it and apply it to generate economic rents" and "is critical to its innovative capabilities."
74. Andrea Back et al., eds., *Getting Real about Knowledge Networks: Unlocking Corporate Knowledge Assets* (New York, NY: Palgrave Macmillan, 2006): 129-143.
75. Dalkir, *Knowledge Management in Theory and Practice*, 190.
76. As inferred in John P. Kotter, *Leading Change* (Boston, MA: Harvard Business School Press, 1996): 10.
77. John P. Kotter and Leonard A. Schlesinger, "Choosing Strategies for Change," in *Organizational Behavior and the Practice of Management*, ed. David R. Hampton, Charles E. Summer, and Ross A. Webber (Glenview, IL: Scott, Foresman and Company, 1983): 735.
78. Hislop, *Knowledge Management in Organizations: A Critical Introduction*, 52.
79. Ibid.
80. Sajda Qureshi, Robert Briggs, and Vlatka Hlupic, "Value Creation from Intellectual Capital: Convergence of Knowledge Management and Collaboration in the Intellectual Bandwidth Model," *Group Decision and Negotiation* 15 (2006): 209.
81. Hislop, *Knowledge Management in Organizations: A Critical Introduction*, 13-37.
82. Ibid., 39.
83. Priestley and Samaddar, "Multi-Organizational Networks: Three Antecedents of Knowledge Transfer," 88. Shared identity or purpose facilitates both intra- and inter-organizational knowledge sharing.
84. Ibid.

85. Patti Anklam, "Knowledge Management: The Collaboration Thread," *Bulletin of the American Society for Information Science and Technology* 28, no. 6 (August - September 2002): 9.

86. Kristen Bell DeTienne, et al., "Toward a Model of Effective Knowledge Management and Directions for Future Research: Culture, Leadership, and CKOs," *Journal of Leadership & Organizational Studies* 10, no. 4 (Spring 2004): 32. See also: Hislop, *Knowledge Management in Organizations: A Critical Introduction*, 90-92.

87. Davenport and Prusak, *Working Knowledge*, 97. See also: Dalkir, *Knowledge Management in Theory and Practice*, 189. Dalkir refers to the fact that mental models are also called basic underlying assumptions and represent possibilities – managers use mental models to "diagnose problems and make decisions."

88. Dalkir, *Knowledge Management in Theory and Practice*, 43.

89. Munoz-Seca and Riverola, *Problem-Driven Management: Achieving Improvement in Operations through Knowledge Management*, 230-231.

90. Nonaka and Takeuchi, *The Knowledge-Creating Company*, 45.

91. Davenport and Prusak, *Working Knowledge*, 97.

92. Gillian Wright and Andrew Taylor, "Strategic Knowledge Sharing for Improved Public Service Delivery: Managing an Innovative Culture for Effective Partnerships," 194-196.

93. Dalkir, *Knowledge Management in Theory and Practice*, 212.

94. Andrew P. Ciganek, En Mao, and Mark Srite, "Organizational Culture for Knowledge Management Systems: A Study of Corporate Users," *International Journal of Knowledge Management* 4, no. 1 (January-March 2008): 5-6.

95. Janice E. Carrillo and Cheryl Gaimon, "Managing Knowledge-Based Resource Capabilities under Uncertainty," *Management Science* 50, no. 11 (November 2004): 1516.

96. Ibid.

97. Davenport and Prusak, *Working Knowledge*, 97.

98. Ibid.

99. Nonaka and Takeuchi, *The Knowledge-Creating Company*, 227.

100. COL Stephen A. Shambach, ed., "Strategic Leadership Tasks," Strategic Leadership Primer, 2nd ed. (Carlisle Barracks, PA: U.S. Army War College, Department of Command, Leadership and Management, 2004): 44.

101. Ibid. See also: Roland K. Yeo, "Building Knowledge Through Action Systems, Process Leadership and Organizational Learning," *Foresight* 8, no. 4 (2006): 37.

102. Ibid., 45. See also: Dalkir, *Knowledge Management in Theory and Practice*, 185.

103. Yeo, "Building Knowledge Through Action Systems, Process Leadership and Organizational Learning," 38. Collaborative cultures with open trans-boundary communication and dialogue foster knowledge sharing based on social construct that leads to systems thinking and shared vision necessary for organizational learning. Wright and Taylor, "Strategic Knowledge Sharing for Improved Public Service Delivery: Managing an Innovative Culture for Effective Partnerships," 203. Innovative cultures encourage knowledge sharing, acquisition, and application that further supports collaboration and learning.
104. Anklam, "Knowledge Management: The Collaboration Thread," 9-10.
105. Shambach, ed., "Strategic Leadership Tasks," 45-46.
106. Dalkir, *Knowledge Management in Theory and Practice*, 3.
107. Information specific to S/CRS is available at: The United States Department of State Office of the Coordinator for Reconstruction and Stabilization Home Page, http://www.state.gov/s/crs/ (accessed February 17, 2009). See also: Farida Hasanali et al., *Communities of Practice: A Guide for your Journey to Knowledge Management Best Practices*, 3.
108. Verna Allee, *The Future of Knowledge: Increasing Prosperity Through Value Networks*, 122-124. See also: Sineenad Paisttanand, L. A. Digman, and Sang M. Lee, "Managing Knowledge Capabilities for Strategy Implementation Effectiveness," *International Journal of Knowledge Management* 3, no. 4 (October-December 2007): 85.
109. Hislop, *Knowledge Management in Organizations: A Critical Introduction*, 58-67.
110. Henrietta Fore, Robert Gates, and Condoleezza Rice, *U.S. Government Counterinsurgency Guid*e (Washington, D.C.: Bureau of Political-Military Affairs, 2009): 19.
111. Peter F. Drucker, *The Essential Drucker* (New York, NY: HarperCollins, 2001): 81.
112. Steven Cavaleri and Sharon Seivert, *Knowledge Leadership: The Art and Science of the Knowledge-Based Organization* (Burlington, MA: Elsevier, Inc., 2005): 269-274. See also: Dr. Kristen Bell DeTienne et al., "Toward a Model of Effective Knowledge Management and Directions for Future Research: Culture, Leadership, and CKOs," 34.
113. Davenport and Prusak, *Working Knowledge*, 5.
114. American Productivity & Quality Center (APQC), *Retaining Valuable Knowledge: Proactive Strategies to Deal With a Shifting Work Force*, 7.
115. Murray E. Jennex, Stefan Smolnik, and David Croasdell, "Knowledge Management Success," *International Journal of Knowledge Management* 3, no. 2 (April-June 2007): ii.

116. Davenport and Prusak, *Working Knowledge*, 169. See also: Aggestam, "Learning Organization or Knowledge Management – Which Came First, The Chicken or the Egg?," 298.

117. Nonaka and Takeuchi, *The Knowledge-Creating Company*, 160-171.

118. Ibid., 166.


Prudens
Futuri